NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61511-1

Première édition
First edition
2003-01

Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le domaine de la production par processus –

Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel

Functional safety – Safety instrumented systems for the process industry sector –

Part 1: Framework, definitions, system, hardware and software requirements

Numéro de référence
Reference number
CEI/IEC 61511-1:2003

Numérotation des publications

Depuis le 1er janvier 1997, les publications de la CEI sont numérotées à partir de 60000. Ainsi, la CEI 34-1 devient la CEI 60034-1.

Editions consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Informations supplémentaires sur les publications de la CEI

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique. Des renseignements relatifs à cette publication, y compris sa validité, sont disponibles dans le Catalogue des publications de la CEI (voir ci-dessous) en plus des nouvelles éditions, amendements et corrigenda. Des informations sur les sujets à l'étude et l'avancement des travaux entrepris par le comité d'études qui a élaboré cette publication, ainsi que la liste des publications parues, sont également disponibles par l'intermédiaire de:

- **Site web de la CEI (www.iec.ch)**
- **Catalogue des publications de la CEI**

  Le catalogue en ligne sur le site web de la CEI (www.iec.ch/searchpub) vous permet de faire des recherches en utilisant de nombreux critères, comprenant des recherches textuelles, par comité d'études ou date de publication. Des informations en ligne sont également disponibles sur les nouvelles publications, les publications remplacées ou retirées, ainsi que sur les corrigenda.
- **IEC Just Published**

  Ce résumé des dernières publications parues (www.iec.ch/online_news/justpub) est aussi disponible par courrier électronique. Veuillez prendre contact avec le Service client (voir ci-dessous) pour plus d'informations.
- **Service clients**

  Si vous avez des questions au sujet de cette publication ou avez besoin de renseignements supplémentaires, prenez contact avec le Service clients:

  Email: custserv@iec.ch
  Tél: +41 22 919 02 11
  Fax: +41 22 919 03 00

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.
- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.
- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

  Email: custserv@iec.ch
  Tel: +41 22 919 02 11
  Fax: +41 22 919 03 00

.

NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
61511-1

Première édition
First edition
2003-01

Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le domaine de la production par processus –

Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel

Functional safety – Safety instrumented systems for the process industry sector –

Part 1: Framework, definitions, system, hardware and software requirements

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE XC

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

CONTENTS

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

SÉCURITÉ FONCTIONNELLE – SYSTÈMES INSTRUMENTÉS DE SÉCURITÉ POUR LE DOMAINE DE LA PRODUCTION PAR PROCESSUS –

Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés «Publication(s) de la CEI»). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme Internationale CEI 61511-1 a été préparée par le Sous-comité 65A: Aspects systèmes, du Comité d'Études 65 de la CEI: Mesure et commande dans les processus industriels.

Cette version bilingue (2003-12) remplace la version monolingue anglaise.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 1: Framework, definitions, system, hardware and software requirements

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61511-1 has been prepared by subcommittee 65A: System aspects, of IEC technical committee 65: Industrial-process measurement and control.

This bilingual version (2003-12) replaces the English version.

Le texte anglais de cette norme est issu des documents 65A/368/FDIS et 65A/372/RVD. Le rapport de vote 65A/372/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

La CEI 61511 comprend les parties suivantes, sous le titre général *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le domaine de la production par processus* (voir la Figure 1).

Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel

Partie 2: Lignes directrices pour l'application de la CEI 61511-1

Partie 3: Guide pour la détermination des niveaux d'intégrité de sécurité requis

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant 2007. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

The text of this standard is based on the following documents:

FDIS	Report on voting
65A/368/FDIS	65A/372/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

The French version of this standard has not been voted upon.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

IEC 61511 consists of the following parts, under the general title *Functional safety: Safety instrumented systems for the process industry sector* (see Figure 1):

Part 1: Framework, definitions, system, hardware and software requirements

Part 2: Guidelines in the application of IEC 61511-1

Part 3: Guidance for the determination of the required safety integrity levels

The committee has decided that the contents of this publication will remain unchanged until 2007. At this date, the publication will be

- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended.

INTRODUCTION

Les systèmes instrumentés de sécurité sont utilisés depuis des années pour exécuter des fonctions instrumentées liées à la sécurité dans les processus industriels. Si l'instrumentation doit être effectivement utilisée pour les fonctions instrumentées liées à la sécurité, il est important que cette instrumentation satisfasse à certaines normes et à certains niveaux minima de performances.

Cette Norme concerne l'application des systèmes instrumentés de sécurité aux industries de production par processus. Elle exige également de conduire une évaluation de danger et de risque des processus pour permettre d'en déduire des spécifications pour les systèmes instrumentés de sécurité. D'autres systèmes de sécurité ne sont considérés que de manière à ce que leur contribution puisse être prise en compte lors de l'examen des exigences de performances concernant les systèmes instrumentés de sécurité. Le système instrumenté de sécurité inclut tous les composants et les sous-ensembles nécessaires pour remplir la fonction instrumentée de sécurité, du (des) capteur(s) à (aux) l'élément(s) terminal(aux).

Cette norme repose sur deux concepts qui sont fondamentaux vis-à-vis de son application: le cycle de vie de sécurité et les niveaux d'intégrité de sécurité.

Cette norme concerne les systèmes instrumentés de sécurité qui sont basés sur l'utilisation d'une technologie électrique/électronique/électronique programmable. Dans le cas où d'autres technologies sont utilisées pour les unités logiques, il convient aussi d'appliquer les principes fondamentaux de cette norme. Cette norme concerne également les capteurs et les éléments terminaux des systèmes instrumentés de sécurité, quelle que soit la technologie utilisée. Cette norme est spécifique de la production industrielle par processus dans le cadre de la CEI 61508 (voir l'Annexe A).

Cette norme présente une approche relative aux activités liées au cycle de vie de sécurité, pour satisfaire à ces normes minimales. Cette approche a été adoptée afin de développer une politique technique rationnelle et cohérente.

Dans la plupart des cas, la meilleure sécurité est obtenue par une conception de processus de sécurité inhérents, chaque fois que cela est possible, combinée, au besoin, avec d'autres systèmes de protection, fondés sur différentes technologies (chimique, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable) et qui couvrent tous les risques résiduels identifiés. Pour faciliter cette approche, cette norme:

- nécessite de réaliser une évaluation des dangers et des risques pour identifier les exigences globales de sécurité;
- exige d'effectuer une allocation des exigences de sécurité au(x) système(s) instrumenté(s) de sécurité;
- s'inscrit dans un cadre applicable à toutes les méthodes instrumentées qui permettent d'obtenir la sécurité fonctionnelle;
- détaille l'utilisation de certaines activités, telles que la gestion de la sécurité, qui peuvent être applicables à toute méthode permettant d'obtenir la sécurité fonctionnelle.

Cette norme sur les systèmes instrumentés de sécurité pour l'industrie de la production par processus:

- prend en compte toutes les phases du cycle de vie de sécurité, depuis le concept initial, en passant par la conception, la mise en oeuvre, l'exploitation et la maintenance, jusqu'au déclassement;
- permet d'harmoniser avec la présente norme les normes spécifiques de processus industriels existantes ou de nouveaux pays.

INTRODUCTION

Safety instrumented systems have been used for many years to perform safety instrumented functions in the process industries. If instrumentation is to be effectively used for safety instrumented functions, it is essential that this instrumentation achieves certain minimum standards and performance levels.

This standard addresses the application of safety instrumented systems for the process industries. It also requires a process hazard and risk assessment to be carried out to enable the specification for safety instrumented systems to be derived. Other safety systems are only considered so that their contribution can be taken into account when considering the performance requirements for the safety instrumented systems. The safety instrumented system includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s).

This standard has two concepts which are fundamental to its application; safety lifecycle and safety integrity levels.

This standard addresses safety instrumented systems which are based on the use of electrical/electronic/programmable electronic technology. Where other technologies are used for logic solvers, the basic principles of this standard should be applied. This standard also addresses the safety instrumented system sensors and final elements regardless of the technology used. This standard is process industry specific within the framework of IEC 61508 (see Annex A).

This standard sets out an approach for safety life-cycle activities to achieve these minimum standards. This approach has been adopted in order that a rational and consistent technical policy is used.

In most situations, safety is best achieved by an inherently safe process design. If necessary, this may be combined with a protective system or systems to address any residual identified risk. Protective systems can rely on different technologies (chemical, mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). To facilitate this approach, this standard

- requires that a hazard and risk assessment is carried out to identify the overall safety requirements;
- requires that an allocation of the safety requirements to the safety instrumented system(s) is carried out;
- works within a framework which is applicable to all instrumented methods of achieving functional safety;
- details the use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety.

This standard on safety instrumented systems for the process industry

- addresses all safety life-cycle phases from initial concept, design, implementation, operation and maintenance through to decommissioning;
- enables existing or new country specific process industry standards to be harmonized with this standard.

Cette norme conduit à un haut niveau de cohérence (par exemple, pour les principes sous-jacents, la terminologie, l'information) au sein des industries de production par processus. Ceci devrait avoir comme conséquence une amélioration en termes de sécurité et d'économie.

Dans les juridictions où des réglementations (par exemple, nationales, fédérales, étatiques, provinciales, du comté, de la ville) sont applicables aux processus de sécurité, à leur conception, à leur gestion, ou à d'autres exigences, ces réglementations sont prioritaires par rapport aux exigences définies dans cette norme.

This International Standard is intended to lead to a high level of consistency (for example, of underlying principles, terminology, information) within the process industries. This should have both safety and economic benefits.

In jurisdictions where the governing authorities (for example, national, federal, state, province, county, city) have established process safety design, process safety management, or other requirements, these take precedence over the requirements defined in this standard.

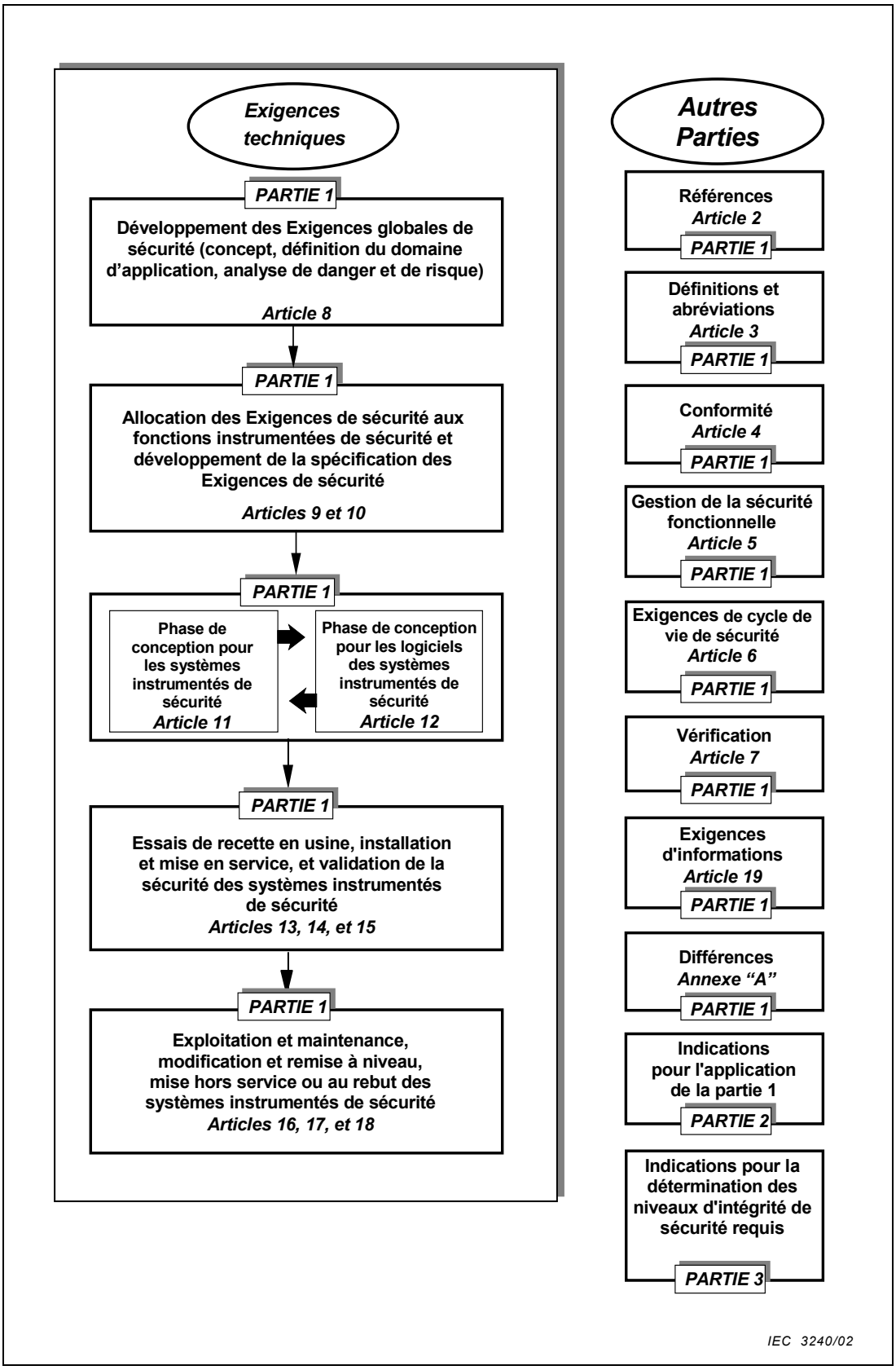


Figure 1 – Structure générale de la présente norme

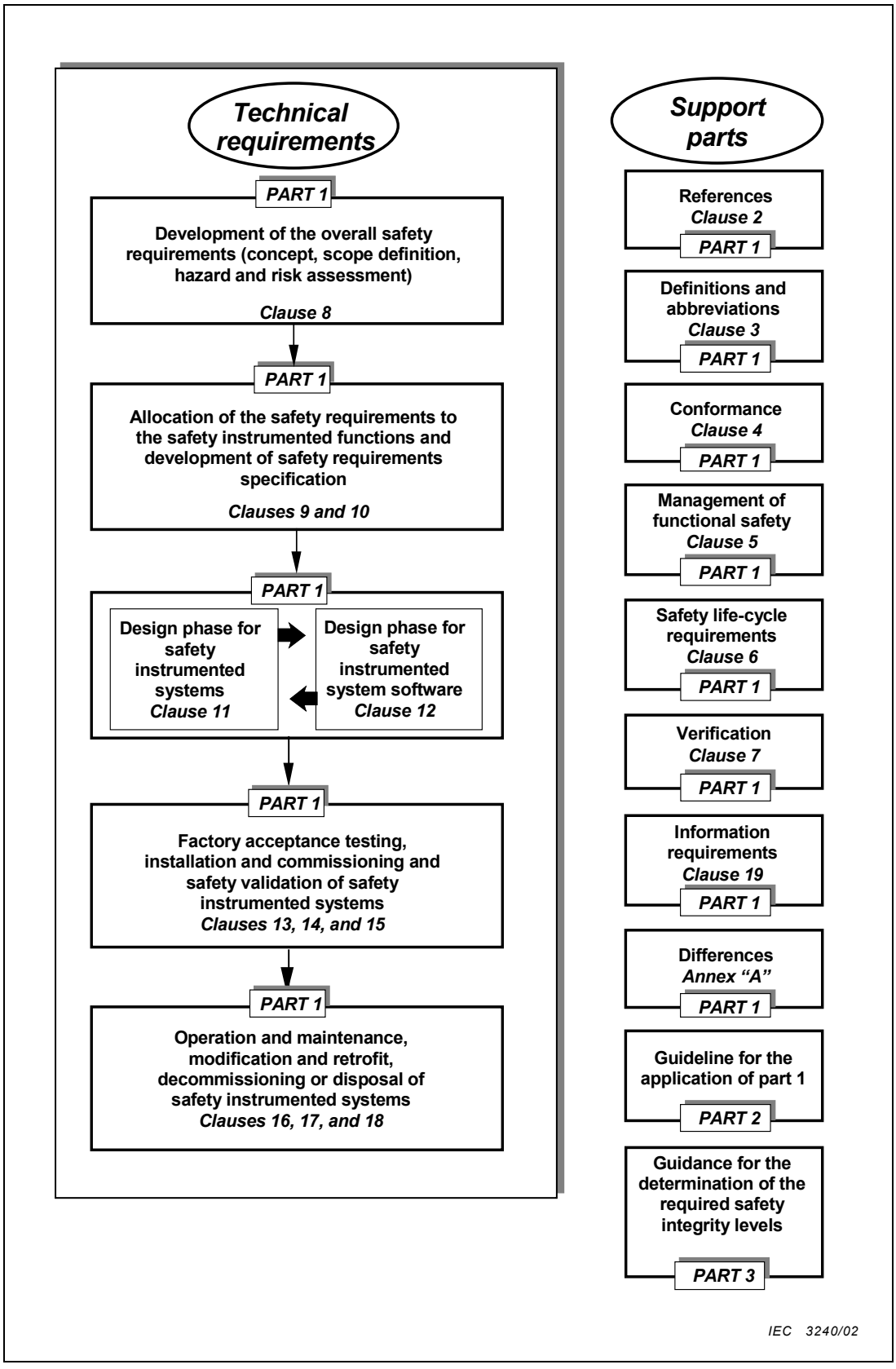


Figure 1 – Overall framework of this standard

SÉCURITÉ FONCTIONNELLE – SYSTÈMES INSTRUMENTÉS DE SÉCURITÉ POUR LE DOMAINE DE LA PRODUCTION PAR PROCESSUS –

Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel

1 Domaine d'application

Cette Norme internationale permet de définir des exigences relatives aux spécifications, à la conception, à l'installation, à l'exploitation et à l'entretien d'un système instrumenté de sécurité, de telle manière qu'il puisse être mis en oeuvre en toute confiance, et ainsi établir et/ou maintenir les processus dans un état de sécurité convenable. La présente norme a été conçue pour être une mise en œuvre de la CEI 61508 dans le domaine de l'industrie des processus.

En particulier, cette norme:

a) spécifie les exigences permettant d'obtenir la sécurité fonctionnelle, mais ne spécifie pas la responsabilité de la mise en oeuvre des exigences (par exemple, les concepteurs, les fournisseurs, la société propriétaire/exploitante, l'entrepreneur); cette responsabilité sera assignée aux différentes parties selon la planification de la sécurité et des règlements nationaux;

b) s'applique lorsque les équipements qui satisfont aux exigences de la CEI 61508, ou de 11.5 de la CEI 61511-1, sont intégrés dans un système global, qui doit être utilisé pour une application dans le domaine des processus; ne s'applique pas aux constructeurs qui déclarent leurs dispositifs comme pouvant être utilisés dans les systèmes instrumentés de sécurité dans le domaine des processus (voir la CEI 61508-2 et la CEI 61508-3);

c) définit les relations entre les normes CEI 61511 et CEI 61508 (Figures 2 et 3);

d) s'applique lorsque le logiciel d'application est développé pour des systèmes ayant une variabilité limitée ou des programmes figés; ne s'applique pas aux constructeurs, aux concepteurs de systèmes instrumentés de sécurité, aux intégrateurs et aux utilisateurs qui développent un logiciel intégré (logiciel système) ou utilisent des langages de variabilité totale (voir la CEI 61508-3);

e) s'applique à de nombreuses industries différentes dans le domaine des processus, comprenant celles des produits chimiques, du raffinage de pétrole, de la production de pétrole et de gaz, de la pâte à papier et du papier, de la production d'électricité non nucléaire;

NOTE Dans le domaine des processus, certaines applications (par exemple, en mer) peuvent avoir des exigences supplémentaires, qui doivent être satisfaites.

f) met en évidence les relations entre les fonctions instrumentées de sécurité et d'autres fonctions (Figure 4);

g) aboutit à l'identification des exigences fonctionnelles et des exigences concernant l'intégrité de sécurité relatives à la (aux) fonction(s) instrumentée(s) de sécurité, en tenant compte de la réduction de risque obtenue par d'autres moyens;

h) spécifie les exigences relatives à l'architecture du système et à la configuration du matériel, au logiciel d'application et à l'intégration du système;

i) spécifie les exigences relatives au logiciel d'application pour les utilisateurs et les intégrateurs des systèmes instrumentés de sécurité (Article 12). En particulier, les exigences pour les points suivants sont spécifiées;

FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 1: Framework, definitions, system, hardware and software requirements

1 Scope

This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard has been developed as a process sector implementation of IEC 61508.

In particular, this standard

a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (for example, designers, suppliers, owner/operating company, contractor); this responsibility will be assigned to different parties according to safety planning and national regulations;

b) applies when equipment that meets the requirements of IEC 61508, or of 11.5 of IEC 61511-1, is integrated into an overall system that is to be used for a process sector application but does not apply to manufacturers wishing to claim that devices are suitable for use in safety instrumented systems for the process sector (see IEC 61508-2 and IEC 61508-3);

c) defines the relationship between IEC 61511 and IEC 61508 (Figures 2 and 3);

d) applies when application software is developed for systems having limited variability or fixed programmes but does not apply to manufacturers, safety instrumented systems designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3);

e) applies to a wide variety of industries within the process sector including chemicals, oil refining, oil and gas production, pulp and paper, non-nuclear power generation;

NOTE Within the process sector some applications, (for example, off-shore), may have additional requirements that have to be satisfied.

f) outlines the relationship between safety instrumented functions and other functions (Figure 4);

g) results in the identification of the functional requirements and safety integrity requirements for the safety instrumented function(s) taking into account the risk reduction achieved by other means;

h) specifies requirements for system architecture and hardware configuration, application software, and system integration;

i) specifies requirements for application software for users and integrators of safety instrumented systems (clause 12). In particular, requirements for the following are specified:

- les phases du cycle de vie de sécurité et les activités qui doivent être mises en oeuvre pendant la conception et le développement du logiciel d'application (modèle de cycle de vie de sécurité du logiciel). Ces exigences incluent l'application de mesures et de techniques, prévues pour éviter des anomalies de logiciel et pour maîtriser les défaillances qui peuvent se produire;
- les informations concernant la validation de la sécurité du logiciel à effectuer vis-à-vis de l'organisme réalisant l'intégration du SIS;
- la préparation des informations et des procédures concernant le(s) logiciel(s) dont l'utilisateur a besoin pour l'exploitation et la maintenance du SIS;
- les procédures et les spécifications à respecter par l'organisme réalisant les modifications du logiciel de sécurité;

j) s'applique lorsque la sécurité fonctionnelle est obtenue en utilisant une ou plusieurs fonctions instrumentées de sécurité, pour la protection du personnel, la protection du public ou la protection de l'environnement;

k) peut être appliqué dans des applications non sécuritaires, telle que la protection des biens;

l) définit des exigences destinées à mettre en oeuvre les fonctions instrumentées de sécurité, faisant partie des dispositions globales pour obtenir la sécurité fonctionnelle;

m) utilise un cycle de vie de sécurité (Figure 8) et définit une liste d'activités, nécessaires pour déterminer les exigences fonctionnelles et les exigences concernant l'intégrité de sécurité, relatives aux systèmes instrumentés de sécurité;

n) prescrit qu'une évaluation de danger et de risque doit être effectuée pour définir les exigences fonctionnelles de sécurité et les niveaux d'intégrité de sécurité de chaque fonction instrumentée de sécurité;

NOTE Voir la Figure 9 pour avoir une vue d'ensemble des méthodes de réduction de risque.

o) établit des objectifs quantitatifs relatifs à la probabilité moyenne de défaillance lors d'une sollicitation et à la probabilité des défaillances dangereuses par heure pour les niveaux d'intégrité de sécurité;

p) spécifie des exigences minimales pour la tolérance aux anomalies du matériel;

q) spécifie les techniques/mesures nécessaires pour obtenir les niveaux d'intégrité spécifiés;

r) définit un niveau maximal de performances (SIL 4), qui peut être atteint pour une fonction instrumentée de sécurité, mise en oeuvre conformément à cette norme;

s) définit un niveau minimal de performances (SIL 1) au-dessous duquel cette norme ne s'applique pas;

t) fournit un cadre pour l'établissement des niveaux d'intégrité de sécurité, mais ne spécifie pas les niveaux d'intégrité de sécurité exigés pour les applications spécifiques (qu'il convient d'établir sur la base de la connaissance de l'application particulière);

u) spécifie les exigences pour toutes les parties du système instrumenté de sécurité, depuis le capteur jusqu'à l'élément terminal ou aux éléments terminaux;

v) définit les informations qui sont nécessaires pendant le cycle de vie de sécurité;

w) prescrit que la conception d'une fonction instrumentée de sécurité tient compte de l'ergonomie;

x) ne met en place aucune prescription directe relative à un opérateur individuel ou à la personne en charge de la maintenance.

- safety life-cycle phases and activities that are to be applied during the design and development of the application software (the software safety life-cycle model). These requirements include the application of measures and techniques, which are intended to avoid faults in the software and to control failures which may occur;
- information relating to the software safety validation to be passed to the organization carrying out the SIS integration;
- preparation of information and procedures concerning software needed by the user for the operation and maintenance of the SIS;
- procedures and specifications to be met by the organization carrying out modifications to safety software;

j) applies when functional safety is achieved using one or more safety instrumented functions for the protection of personnel, protection of the general public or protection of the environment;

k) may be applied in non-safety applications such as asset protection;

l) defines requirements for implementing safety instrumented functions as a part of the overall arrangements for achieving functional safety;

m) uses a safety life cycle (Figure 8) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the safety instrumented systems;

n) requires that a hazard and risk assessment is to be carried out to define the safety functional requirements and safety integrity levels of each safety instrumented function;

NOTE See Figure 9 for an overview of risk reduction methods.

o) establishes numerical targets for average probability of failure on demand and frequency of dangerous failures per hour for the safety integrity levels;

p) specifies minimum requirements for hardware fault tolerance;

q) specifies techniques/measures required for achieving the specified integrity levels;

r) defines a maximum level of performance (SIL 4) which can be achieved for a safety instrumented function implemented according to this standard;

s) defines a minimum level of performance (SIL 1) below which this standard does not apply;

t) provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications (which should be established based on knowledge of the particular application);

u) specifies requirements for all parts of the safety instrumented system from sensor to final element(s);

v) defines the information that is needed during the safety life cycle;

w) requires that the design of a safety instrumented function takes into account human factors;

x) does not place any direct requirements on the individual operator or maintenance person.

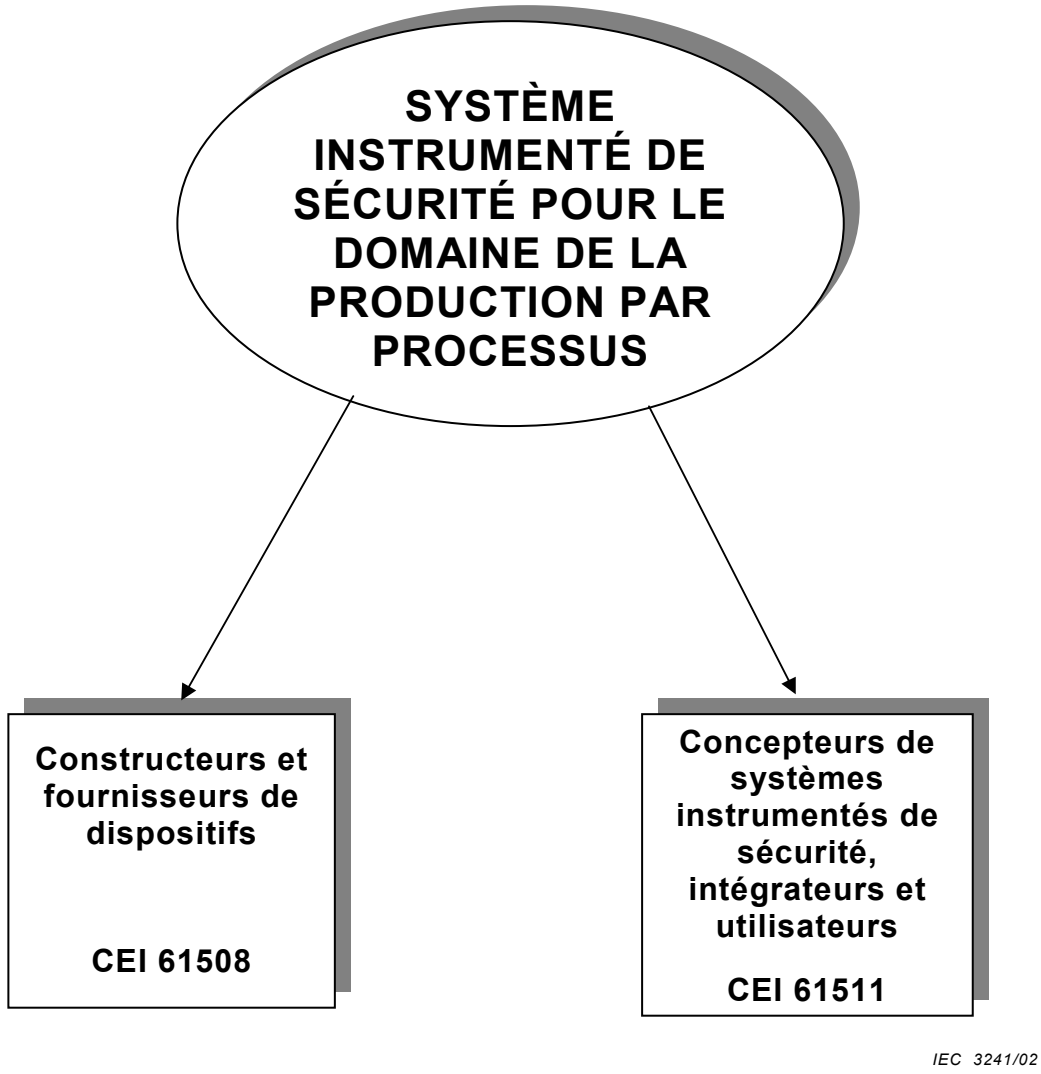


Figure 2 – Relations entre la CEI 61511 et la CEI 61508

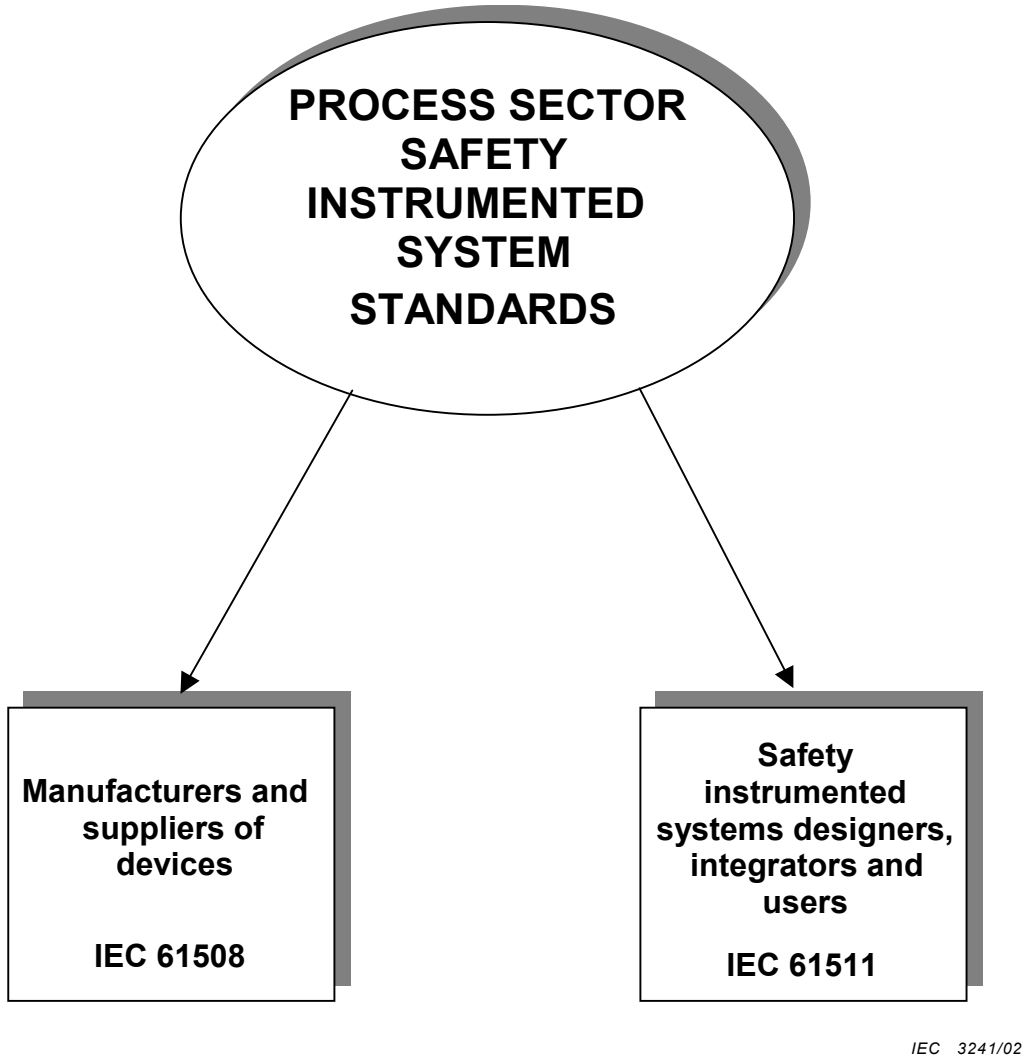
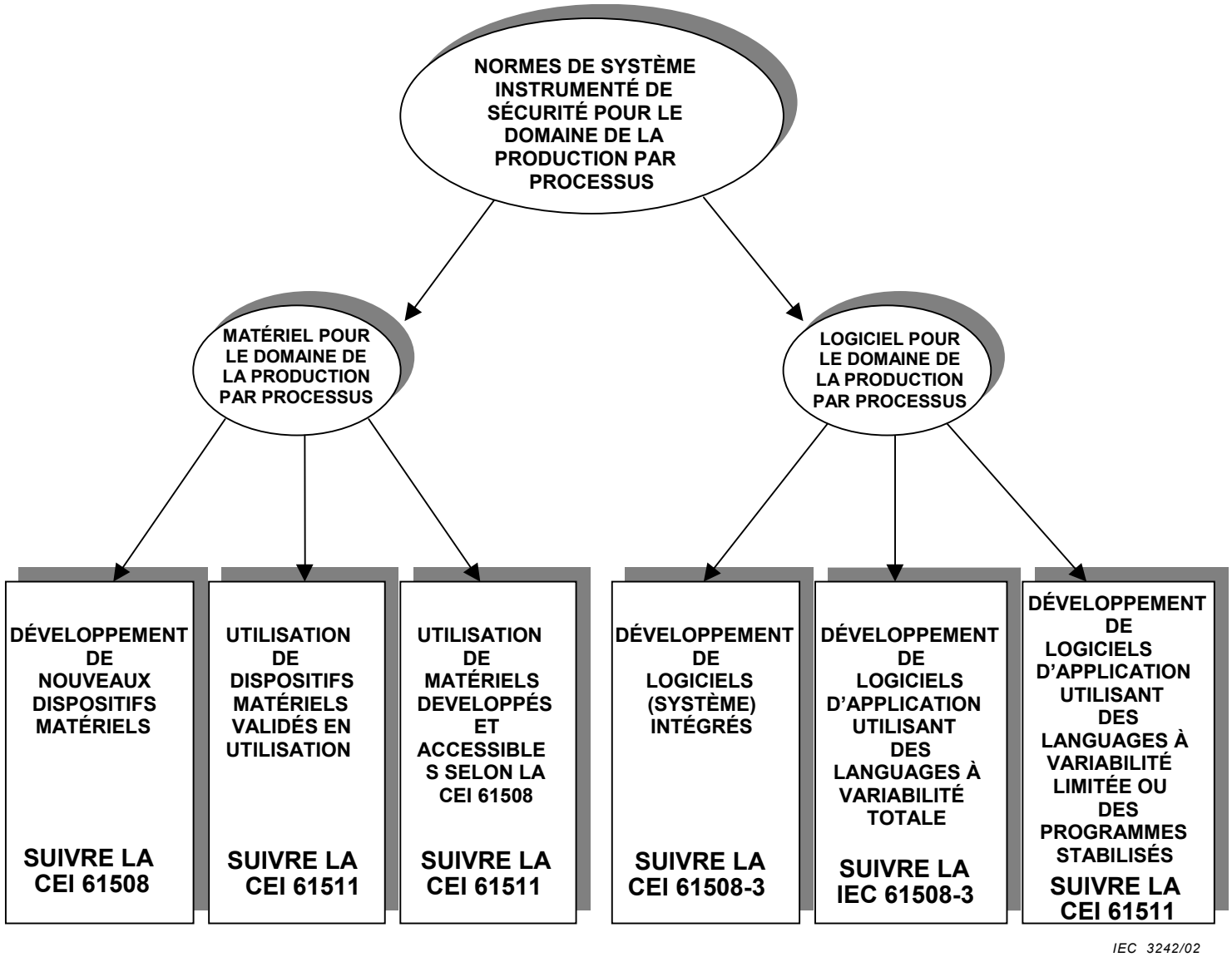


Figure 2 – Relationship between IEC 61511 and IEC 61508



IEC 3242/02

Figure 3 – Relations entre la CEI 61511 et la CEI 61508 (voir Article 1)

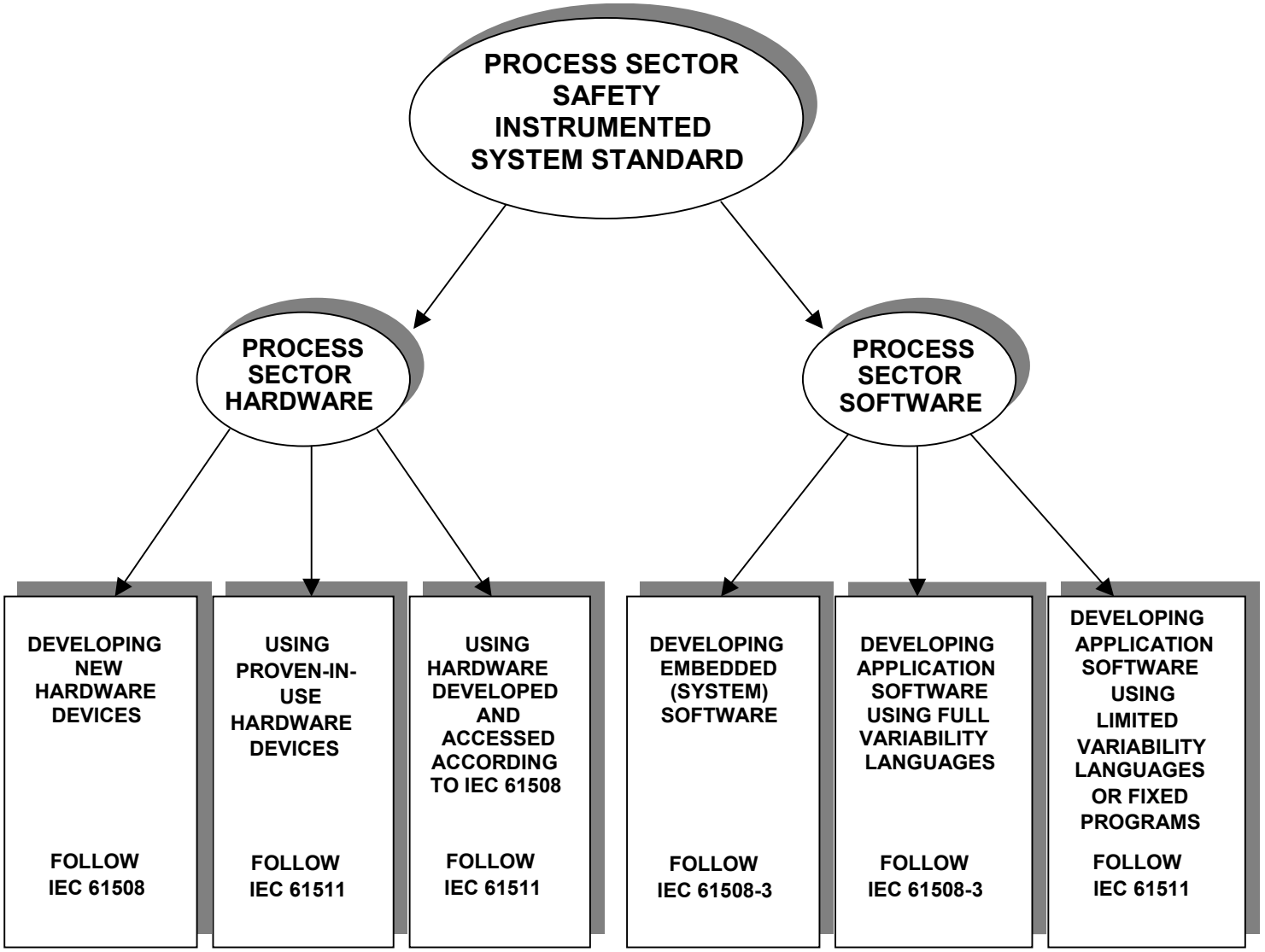


Figure 3 – Relationship between IEC 61511 and IEC 61508 (see clause 1)

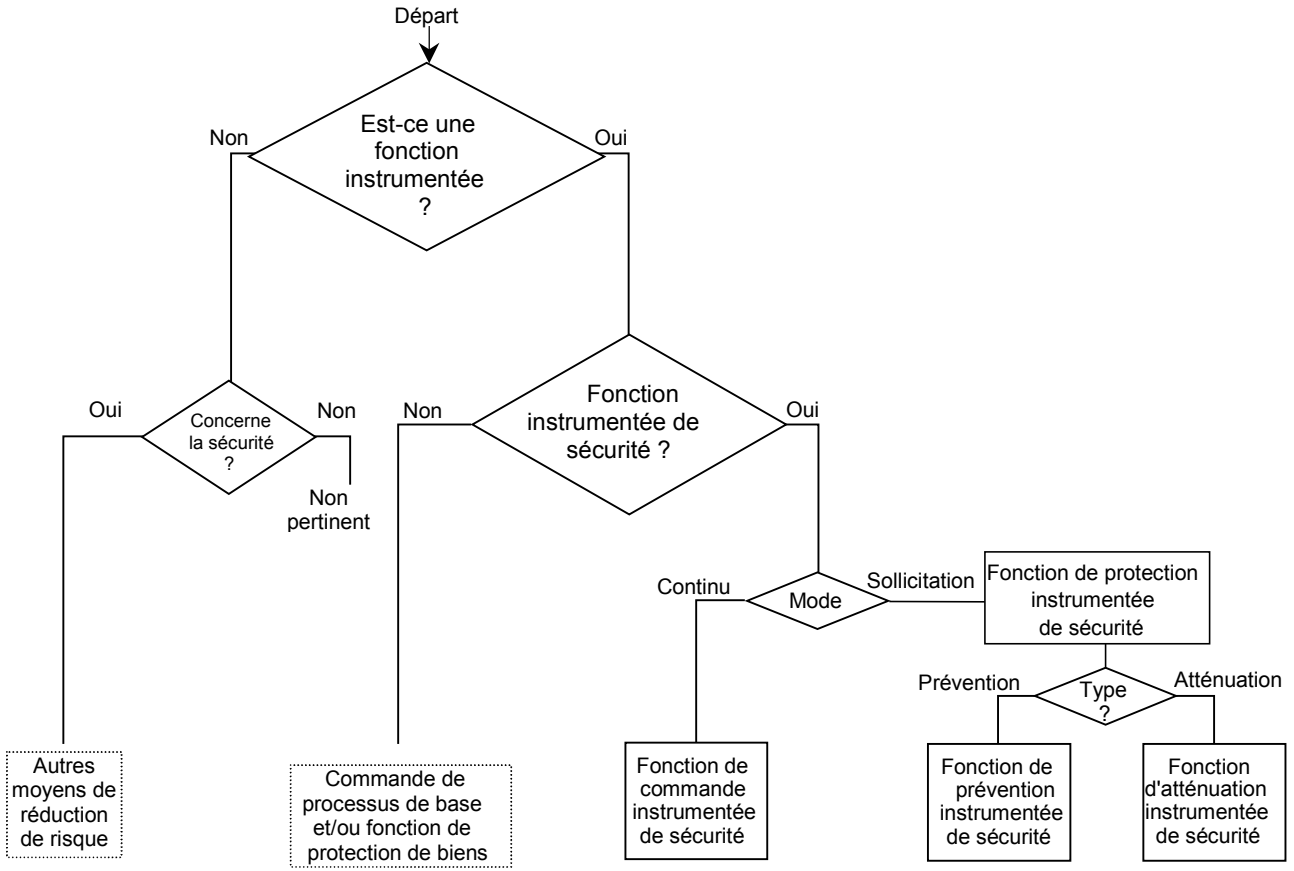


Figure 4 – Relations entre les fonctions instrumentées de sécurité et les autres fonctions

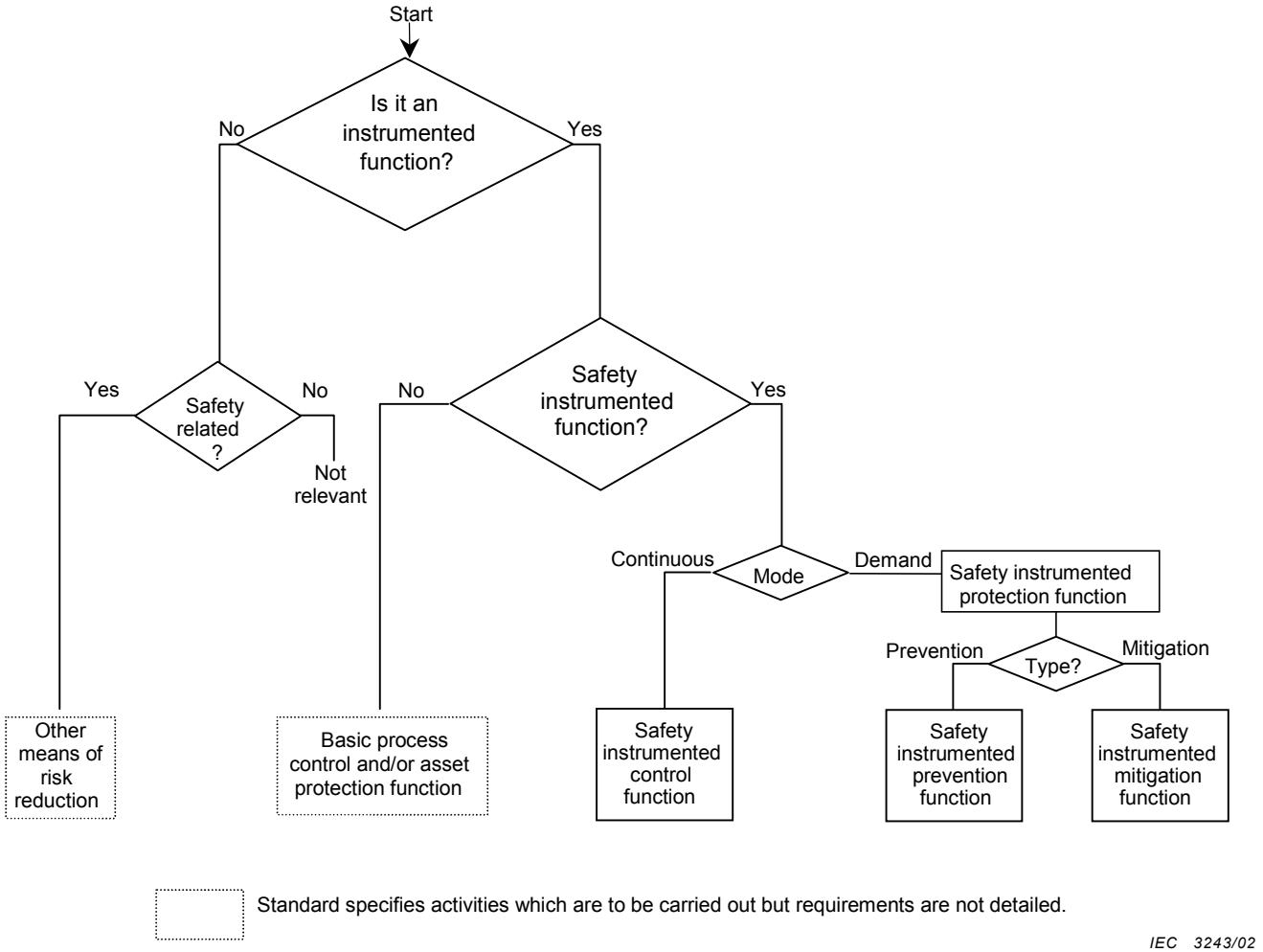


Figure 4 – Relationship between safety instrumented functions and other functions

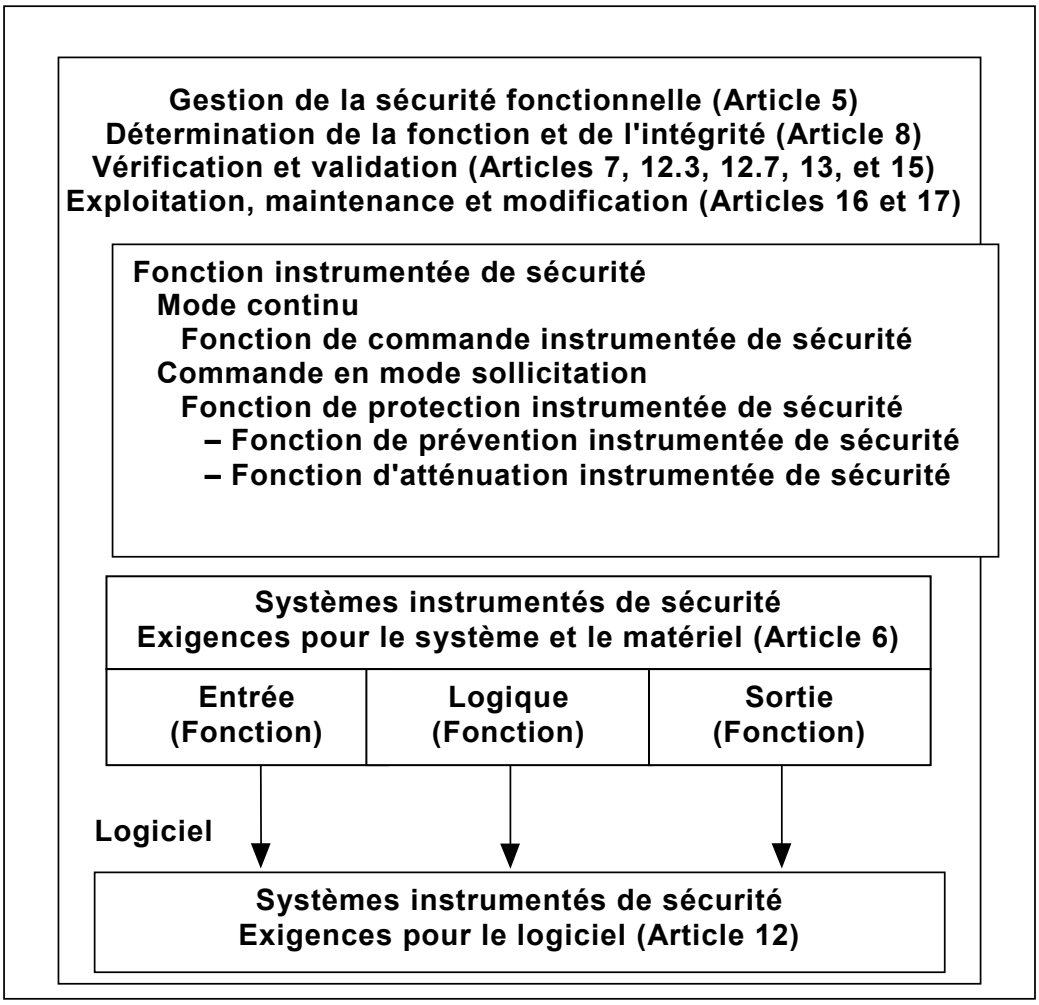
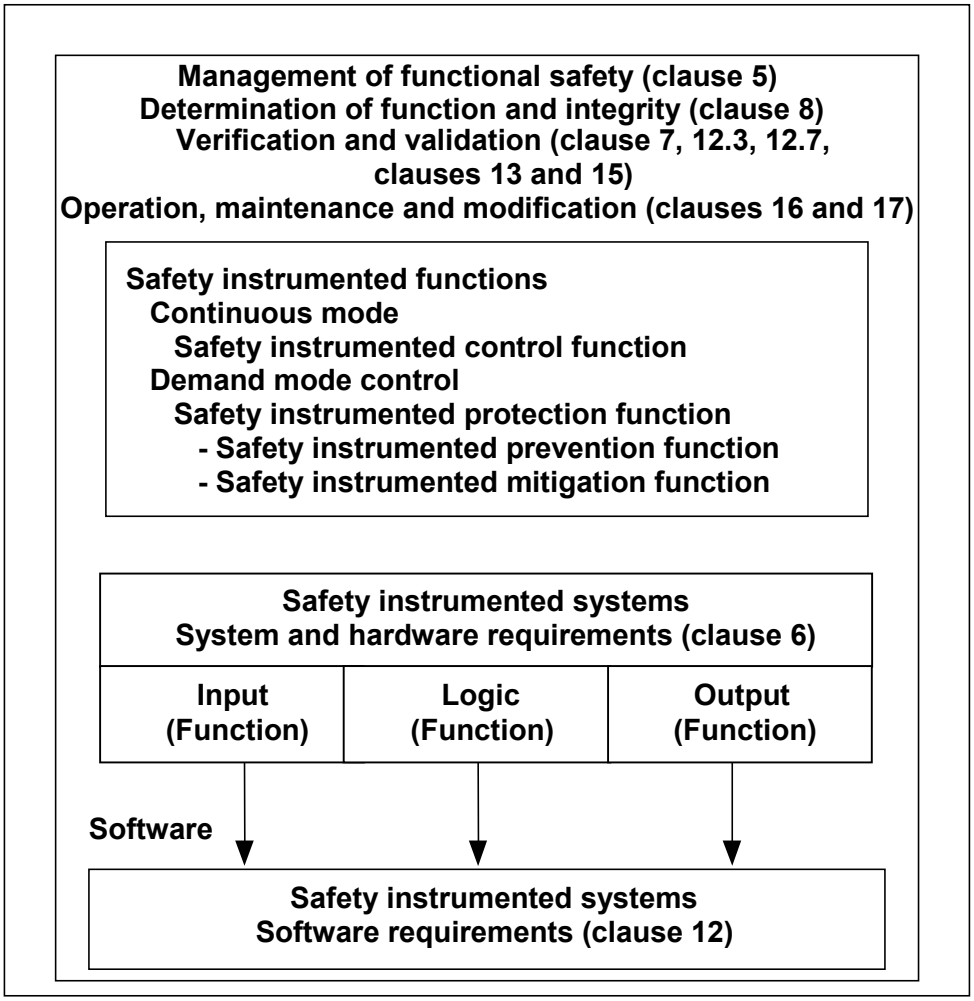


Figure 5 – Relations entre le système, le matériel, et le logiciel dans la CEI 61511-1



IEC 3244/02

Figure 5 – Relationship between system, hardware, and software of IEC 61511-1

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60654-1:1993, *Matériels de mesure et de commande dans les processus industriels – Conditions de fonctionnement – Partie 1: Conditions climatiques*

CEI 60654-3:1998, *Matériels de mesure et de commande dans les processus industriels – Conditions de fonctionnement – Partie 3:Influences mécaniques*

CEI 61326-1, *Matériels électriques de mesure, de commande et de laboratoire – Prescriptions relatives à la CEM – Partie 1: Prescriptions générales*

CEI 61508-2, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

CEI 61508-3, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels*

CEI 61511-2, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le domaine de la production par processus – Partie 2: Lignes directrices pour l'application de la CEI 61511-1*

3 Abréviations et définitions

3.1 Abréviations

Les abréviations utilisées dans l'ensemble de la CEI 61511 sont données dans le Tableau 1.

Tableau 1 – Abréviations utilisées dans la CEI 61511

Abréviation	Expression complète en anglais	Expression complète en français
AC/DC	Alternating current/direct current	Courant alternatif/Courant continu
ALARP	As low as reasonably practicable	Aussi faible que raisonnablement possible
ANSI	American National Standards Institute	Organisme national de normalisation américain
BPCS	Basic process control system	Système de commande de processus de base
DC	Diagnostic coverage	Couverture du diagnostic
E/E/PE	Electrical/electronic/programmable electronic	Électrique/électronique/électronique programmable
E/E/PES	Electrical/electronic/programmable electronic system	Système électrique/électronique/électronique programmable
EMC	Electro–magnetic compatibility	Compatibilité électromagnétique
FAT	Factory acceptance testing	Essais de recette en usine
FPL	Fixed program language	Langage de programme figé
FTA	Fault tree analysis	Analyse par arbre de panne
FVL	Full variability language	Langage de variabilité totale
HFT	Hardware fault tolerance	Tolérance aux anomalies du matériel
HMI	Human machine interface	Interface homme-machine (IHM)
H & RA	Hazard & risk analysis	Analyse de danger et de risque
HRA	Human reliability analysis	Analyse de fiabilité humaine
H/W	Hardware	Matériel

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60654-1:1993, *Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions*

IEC 60654-3:1998, *Industrial-process measurement and control equipment – Operating conditions – Part 3: Mechanical influences*

IEC 61326-1:*Electrical equipment for measurement, control and laboratory use – EMC requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61511-2: *Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines in the application of IEC 61511-1*

3 Abbreviations and definitions

3.1 Abbreviations

Abbreviations used throughout IEC 61511 are given in Table 1.

Table 1 – Abbreviations used in IEC 61511

Abbreviation	Full expression
AC/DC	Alternating current/direct current
ALARP	As low as reasonably practicable
ANSI	American National Standards Institute
BPCS	Basic process control system
DC	Diagnostic coverage
E/E/PE	Electrical/electronic/programmable electronic
E/E/PES	Electrical/electronic/programmable electronic system
EMC	Electro-magnetic compatibility
FAT	Factory acceptance testing
FPL	Fixed program language
FTA	Fault tree analysis
FVL	Full variability language
HFT	Hardware fault tolerance
HMI	Human machine interface
H&RA	Hazard and risk assessment
HRA	Human reliability analysis
H/W	Hardware

Abréviation	Expression complète en anglais	Expression complète en français
IEC	International Electrotechnical Commission	Commission Électrotechnique Internationale (CEI)
IEV	International Electrotechnical Vocabulary	Vocabulaire Électrotechnique International (VEI)
ISA	Instrumentation, Systems and Automation Society	Association internationale de normalisation
ISO	International Organization for Standardization	Organisation internationale de normalisation
LVL	Limited variability language	Langage de variabilité limitée
MooN	«M» out of «N» (see 3.2.45)	Architecture M canaux parmi N (voir 3.2.45)
NP	Non-programmable	Non programmable
PE	Programmable electronics	Électronique programmable
PES	Programmable electronic system	Système électronique programmable
PFD	Probability of failure on demand	Probabilité de défaillance lors d'une sollicitation
PFD_{avg}	Average probability of failure on demand	Probabilité moyenne de défaillance lors d'une sollicitation
PLC	Programmable logic controller	Automate programmable
SAT	Site acceptance test	Essai de recette sur site
SFF	Safe failure fraction	Proportion de défaillances en sécurité
SIF	Safety instrumented function	Fonction instrumentée de sécurité
SIL	Safety integrity level	Niveau d'intégrité de sécurité
SIS	Safety instrumented system	Système instrumenté de sécurité
SRS	Safety requirement specification	Spécification des exigences concernant la sécurité
S/W	Software	Logiciel

3.2 Définitions

Pour les besoins du présent document, les définitions suivantes s'appliquent.

3.2.1
architecture
configuration des éléments matériels et/ou logiciels dans un système, par exemple:

(1) agencement des sous-systèmes du système (SIS) instrumenté de sécurité;

(2) structure interne d'un sous-système de SIS;

(3) agencement des programmes du logiciel

NOTE Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.2
protection de biens
fonction allouée à la conception du système dans le but de prévenir la perte de biens

3.2.3
système de commande de processus de base (BPCS)
système qui répond aux signaux d'entrée provenant du processus, de ses équipements associés, d'autres systèmes programmables et/ou d'un opérateur, et qui génère des signaux de sortie faisant fonctionner le processus et ses équipements associés de la manière souhaitée, mais qui n'exécute aucune fonction instrumentée de sécurité avec un SIL annoncé ≥ 1

NOTE Voir Article A.2.

IEC	International Electrotechnical Commission
IEV	International Electrotechnical Vocabulary
ISA	Instrumentation, Systems and Automation Society
ISO	International Organization for Standardization
LVL	Limited variability language
MooN	"M" out of "N" (see 3.2.45)
NP	Non-programmable
PE	Programmable electronics
PES	Programmable electronic system
PFD	Probability of failure on demand
PFD_{avg}	Average probability of failure on demand
PLC	Programmable logic controller
SAT	Site acceptance test
SFF	Safe failure fraction
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SRS	Safety requirement specification
S/W	Software

3.2 Definitions

For the purposes of this document, the following definitions apply.

3.2.1
architecture
arrangement of hardware and/or software elements in a system, for example,

(1) arrangement of safety instrumented system (SIS) subsystems;

(2) internal structure of an SIS subsystem;

(3) arrangement of software programs

NOTE This term differs from the definition in IEC 61508-4 to reflect differences in the process sector terminology.

3.2.2
asset protection
function allocated to system design for the purpose of preventing loss to assets

3.2.3
basic process control system (BPCS)
system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1

NOTE See Clause A.2.

3.2.4
canal
élément ou groupe d'éléments exécutant une fonction indépendante

NOTE 1 Les éléments d'un canal peuvent comporter des modules d'entrée et de sortie (E/S), des systèmes logiques (voir 3.2.40), des capteurs et des éléments terminaux.

NOTE 2 Une configuration à double canal (à deux canaux) comprend deux canaux réalisant indépendamment la même fonction.

NOTE 3 Ce terme peut être utilisé pour décrire un système complet ou une partie seulement d'un système (par exemple les capteurs ou les éléments terminaux).

3.2.5
codage
voir «programmation»

3.2.6
3.2.6.1
défaillance de cause commune
défaillance résultant d'un ou plusieurs événements qui, en provoquant des défaillances simultanées de deux ou plusieurs canaux séparés dans un système multi-canal, conduit à la défaillance du système

3.2.6.2
défaillance de mode commun
défaillance de deux canaux ou plus, de même origine, provoquant le même résultat erroné

3.2.7
composant
une des parties d'un système, d'un sous-système ou d'un dispositif, exécutant une fonction spécifique

3.2.8
configuration
voir «architecture»

3.2.9
gestion de configuration
discipline d'identification des composants d'un système évolutif (matériel et logiciel) ayant pour objectif de maîtriser les modifications de ces composants et de maintenir la continuité et la traçabilité tout au long du cycle de vie

3.2.10
système de commande
système qui réagit à des signaux d'entrée provenant du processus et/ou d'un opérateur et qui produit des signaux de sortie qui font que le processus fonctionne de la manière souhaitée

NOTE Le système de commande comprend des dispositifs d'entrée et des éléments terminaux et peut être soit un BPCS, soit un SIS ou une combinaison des deux.

3.2.11
défaillance dangereuse
défaillance qui a la potentialité de mettre le système instrumenté de sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

NOTE Le fait que cette potentialité se réalise ou non peut dépendre de l'architecture de canal du système; pour les systèmes ayant plusieurs canaux destinés à accroître la sécurité, il est moins probable qu'une défaillance dangereuse du matériel conduise à un état dangereux de l'ensemble ou à un état dans lequel la fonction ne peut plus être exécutée.

3.2.4
channel
element or group of elements that independently perform(s) a function

NOTE 1 The elements within a channel could include input/output (I/O) modules, logic systems (see 3.2.40), sensors, final elements.

NOTE 2 A dual channel (i.e., a two-channel) configuration is one with two channels that independently perform the same function.

NOTE 3 The term can be used to describe a complete system or a portion of a system (for example, sensors or final elements).

3.2.5
coding
see “programming”

3.2.6

3.2.6.1
common cause failure
failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure

3.2.6.2
common mode failure
failure of two or more channels in the same way, causing the same erroneous result

3.2.7
component
one of the parts of a system, subsystem, or device performing a specific function

3.2.8
configuration
see “architecture”

3.2.9
configuration management
discipline of identifying the components of an evolving (hardware and software) system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the life cycle

3.2.10
control system
system which responds to input signals from the process and/or from an operator and generates output signals causing the process to operate in the desired manner

NOTE The control system includes input devices and final elements and may be either a BPCS or an SIS or a combination of the two.

3.2.11
dangerous failure
failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state

NOTE Whether or not the potential is realized may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a dangerous hardware failure is less likely to lead to the overall hazardous or fail-to-function state.

3.2.12
défaillance dépendante
défaillance dont la probabilité ne peut être exprimée en tant que simple produit des probabilités non conditionnelles de chacun des événements individuels qui l'ont provoquée

NOTE 1 Deux événements A et B sont dépendants, *P*(z) étant la probabilité de l'événement z, seulement si: *P*(A et B) > *P*(A) × *P*(B).

NOTE 2 Voir 9.5 comme exemple de considération de défaillance dépendante entre des couches de protection.

NOTE 3 Les défaillances dépendantes incluent la cause commune – voir 3.2.6.

3.2.13
détecté
révélé
déclaré
se rapporte aux défaillances de matériel et anomalies de logiciel, détectées par les tests de diagnostic, ou lors de l'exploitation normale

3.2.14
dispositif
unité fonctionnelle de matériel ou de logiciel, ou les deux, capable d'accomplir une mission spécifiée (par exemple, dispositifs sur le terrain; équipements connectés, côté utilisation, aux bornes d'E/S d'un SIS; de tels équipements incluent le câblage sur le terrain, les capteurs, les éléments terminaux, les unités logiques, et les dispositifs d'interface avec l'opérateur, câblés par fils aux bornes des E/S du SIS)

3.2.15
couverture du diagnostic (DC)
la couverture du diagnostic d'un composant ou d'un sous-système est le rapport du taux des défaillances détectées au taux des défaillances totales du composant ou du sous-système détectées par les tests de diagnostic. La couverture du diagnostic ne comprend aucune anomalie détectée par les tests périodiques

NOTE 1 La couverture du diagnostic est utilisée pour calculer les taux des défaillances détectées (λ_D) et non détectées (λ_U) à partir du taux des défaillances totales (λ_T), de la manière suivante: λ_D = DC x λ_T et λ_U = (1-DC) x λ_T .

NOTE 2 La couverture du diagnostic est appliquée aux composants ou aux sous-systèmes d'un système instrumenté de sécurité. Par exemple, la couverture du diagnostic est communément déterminée pour un capteur, un élément terminal ou une unité logique.

NOTE 3 En ce qui concerne les applications de sécurité, la couverture du diagnostic est habituellement appliquée aux défaillances en sécurité et aux défaillances dangereuses d'un composant ou d'un sous-système. Par exemple la couverture du diagnostic pour des défaillances dangereuses d'un composant ou d'un sous-système est DC = $\lambda_{DD}/\lambda_{DT}$, où λ_{DD} est le taux des défaillances dangereuses détectées et λ_{DT} est le taux des défaillances dangereuses totales.

3.2.16
diversité
existence de moyens différents pour réaliser une fonction requise

NOTE La diversité peut être atteinte par des méthodes physiques différentes ou par des approches de conception différentes.

3.2.17
électrique/électronique/électronique programmable (E/E/PE)
technologie basée sur les techniques électrique (E), et/ou électronique (E) et/ou électronique programmable (PE)

NOTE Ce terme est censé couvrir l'ensemble des dispositifs ou systèmes fonctionnant selon des principes électriques, et qui pourraient comprendre:

– les dispositifs électromécaniques (électriques);

– les dispositifs électroniques non programmables à circuits intégrés (électroniques);

– les dispositifs électroniques basés sur la technologie informatique (électroniques programmables) – voir 3.2.55.

3.2.12
dependent failure
failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events which caused it

NOTE 1 Two events A and B are dependent, where P(z) is the probability of event z, only if P(A and B) > P(A) × P(B).

NOTE 2 See 9.5 as an example of dependent failure consideration between layers of protection.

NOTE 3 Dependent failure includes common cause (see 3.2.6).

3.2.13
detected
revealed
overt
in relation to hardware failures and software faults, detected by the diagnostic tests or through normal operation

3.2.14
device
functional unit of hardware or software, or both, capable of accomplishing a specified purpose (for example, field devices; equipment connected to the field side of the SIS I/O terminals; such equipment includes field wiring, sensors, final elements, logic solvers, and those operator interface devices hard-wired to SIS I/O terminals)

3.2.15
diagnostic coverage (DC)
ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic tests. Diagnostic coverage does not include any faults detected by proof tests.

NOTE 1 The diagnostic coverage is used to compute the detected ($\lambda_{detected}$) and undetected failure rates ($\lambda_{undected}$) from the total failure rate ($\lambda_{total\ failure\ rate}$) as follows: $\lambda_{detected} = DC \times \lambda_{total\ failure\ rate}$ and $\lambda_{undected} = (1\text{-}DC) \times \lambda_{total\ failure\ rate}$.

NOTE 2 Diagnostic coverage is applied to components or subsystems of a safety instrumented system. For example, the diagnostic coverage is typically determined for a sensor, final element or a logic solver.

NOTE 3 For safety applications the diagnostic coverage is typically applied to the safe and dangerous failures of a component or subsystem. For example, the diagnostic coverage for the dangerous failures of a component or subsystem is $DC = \lambda_{DD}/\lambda_{DT}$, where λ_{DD} is the dangerous detected failure rate and λ_{DT} is the total dangerous failure rate.

3.2.16
diversity
existence of different means performing a required function

NOTE Diversity may be achieved by different physical methods or different design approaches.

3.2.17
electrical/electronic/programmable (E/E/PE)
based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

NOTE The term is intended to cover any and all devices or systems operating on electrical principles and would include

– electro-mechanical devices (electrical);

– solid-state non-programmable electronic devices (electronic);

– electronic devices based on computer technology (programmable electronic) (see 3.2.55).

3.2.18
erreur
écart ou discordance entre une valeur ou une condition calculée, observée ou mesurée, et la valeur ou la condition vraie, prescrite ou théoriquement correcte

NOTE Adapté du VEI 191-05-24, en excluant les notes.

3.2.19
dispositifs externes de réduction de risque
mesures destinées à réduire ou atténuer les risques qui sont séparés et distincts du SIS

NOTE 1 Par exemple, un système de drainage, une cloison coupe-feu, une digue de sécurité.

NOTE 2 Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.20
défaillance
cessation de l'aptitude d'une unité fonctionnelle à accomplir une fonction requise

NOTE 1 Cette définition (en excluant les notes) correspond à l'ISO/CEI 2382-14-01-09.

NOTE 2 Pour de plus amples informations, voir la CEI 61508-4.

NOTE 3 L'accomplissement d'une fonction requise exclut nécessairement certains comportements, et certaines fonctions peuvent être spécifiées en termes de comportements à éviter. L'occurrence d'un comportement à éviter est une défaillance.

NOTE 4 Les défaillances sont soit aléatoires, soit systématiques (voir 3.2.62 et 3.2.85).

3.2.21
anomalie
condition anormale qui peut entraîner une réduction de capacité ou la perte de capacité d'une unité fonctionnelle à accomplir une fonction requise

NOTE Le VEI 191-05-01 définit «fault» (en français «panne») comme un état d'inaptitude à accomplir une fonction requise, en excluant l'inaptitude due à la maintenance préventive, à d'autres actions programmées ou à un manque de ressources extérieures. [ISO/CEI 2382-14-01-09]

3.2.22
évitement des anomalies
utilisation de techniques et procédures destinées à éviter l'apparition d'anomalies durant chacune des phases du cycle de vie de sécurité du système instrumenté de sécurité

3.2.23
tolérance aux anomalies
aptitude d'une unité fonctionnelle à continuer d'accomplir une fonction requise en présence d'anomalies ou d'erreurs

NOTE La définition du terme «tolérant aux pannes» dans le VEI 191-15-05 ne prend en compte que les pannes de sous entités. Voir la note du terme «anomalie» en 3.2.21.

[ISO/CEI 2382-14-04-06]

3.2.24
élément terminal
partie d'un système instrumenté de sécurité qui met en œuvre l'action physique nécessaire pour obtenir un état de sécurité

NOTE Des exemples sont: vannes, dispositifs de commutation, moteurs comprenant leurs éléments auxiliaires, par exemple, une électrovalve et un actionneur, s'ils sont impliqués dans une fonction instrumentée de sécurité.

3.2.25
sécurité fonctionnelle
sous-ensemble de la sécurité globale se rapportant au processus et au BPCS, qui dépend du fonctionnement correct du SIS et d'autres couches de protection

NOTE Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.18
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

NOTE Adapted from IEV 191-05-24 by excluding the notes.

3.2.19
external risk reduction facilities
measures to reduce or mitigate the risks, which are separate and distinct from the SIS

NOTE 1 Examples include a drain system, fire wall, bund (dike).

NOTE 2 This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector terminology.

3.2.20
failure
termination of the ability of a functional unit to perform a required function

NOTE 1 This definition (excluding these notes) matches ISO/IEC 2382-14-01-09:1997.

NOTE 2 For further information, see IEC 61508-4.

NOTE 3 Performance of required functions necessarily excludes certain behaviour, and some functions may be specified in terms of behaviour to be avoided. The occurrence of such behaviour is a failure.

NOTE 4 Failures are either random or systematic (see 3.2.62 and 3.2.85).

3.2.21
fault
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function

NOTE IEV 191-05-01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources. [ISO/IEC 2382-14-01-09]

3.2.22
fault avoidance
use of techniques and procedures which aim to avoid the introduction of faults during any phase of the safety life cycle of the safety instrumented system

3.2.23
fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors

NOTE The definition in IEV 191-15-05 refers only to sub-item faults. See the note for the term fault in 3.2.21.

[ISO/IEC 2382-14-04-06]

3.2.24
final element
part of a safety instrumented system which implements the physical action necessary to achieve a safe state

NOTE Examples are valves, switch gear, motors including their auxiliary elements, for example, a solenoid valve and actuator if involved in the safety instrumented function.

3.2.25
functional safety
part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers

NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.26
évaluation de la sécurité fonctionnelle
recherche, à partir de preuves, destinée à juger de l'état de sécurité fonctionnelle atteint par une ou plusieurs couches de protection

NOTE Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.27
audit de la sécurité fonctionnelle
examen systématique et indépendant destiné à déterminer si les procédures spécifiques aux exigences sur la sécurité fonctionnelle sont conformes aux procédures prévues, sont effectivement mises en œuvre et permettent d'atteindre les objectifs spécifiés

NOTE Un audit de la sécurité fonctionnelle peut être mené dans le cadre d'une évaluation de la sécurité fonctionnelle.

3.2.28
unité fonctionnelle
entité matérielle ou logicielle, ou les deux à la fois, capable de remplir une fonction déterminée

NOTE 1 Dans le VEI 191-01-01, le terme «entité» est employé à la place d'unité fonctionnelle. Une entité peut, dans certains cas, comprendre du personnel.

NOTE 2 C'est la définition donnée par l'ISO/CEI 2382-14-01-01.

3.2.29
intégrité de sécurité du matériel
partie de l'intégrité de sécurité de la fonction instrumentée de sécurité liée aux défaillances aléatoires du matériel en mode de défaillance dangereux

NOTE 1 Le terme fait référence aux défaillances en mode dangereux. C'est-à-dire les défaillances d'une fonction instrumentée de sécurité qui seraient susceptibles de nuire à son intégrité de sécurité. Les deux paramètres à prendre en compte en l'occurrence sont le taux global des défaillances dangereuses et la probabilité de défaillance du fonctionnement lors d'une sollicitation.

NOTE 2 Voir 3.2.86.

NOTE 3 Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.30
dommage
blessure physique ou atteinte à la santé affectant des personnes soit directement, soit indirectement, comme conséquence à un dégât causé aux biens ou à l'environnement

NOTE Cette définition correspond au Guide ISO/CEI 51.

3.2.31
phénomène dangereux
source potentielle de danger

NOTE 1 Cette définition (sans les notes) correspond à 3.4 du Guide ISO/CEI 51.

NOTE 2 Ce terme comprend le danger sur des personnes survenant dans un court laps de temps (par exemple, feu ou explosion), et aussi le danger à long terme sur la santé d'une personne (par exemple, dégagement d'une substance toxique).

3.2.32
erreur humaine
faute
action humaine ou absence d'intervention, qui produit un résultat non recherché

NOTE C'est la définition trouvée dans l'ISO/CEI 2382-14-02-03 et qui diffère de celle donnée dans le VEI 191-05-25 par l'ajout de «ou absence d'intervention».

3.2.26
functional safety assessment
investigation, based on evidence, to judge the functional safety achieved by one or more protection layers

NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.27
functional safety audit
systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives

NOTE A functional safety audit may be carried out as part of a functional safety assessment.

3.2.28
functional unit
entity of hardware or software, or both, capable of accomplishing a specified purpose

NOTE 1 In IEV 191-01-01 the more general term “item” is used in place of functional unit. An item may sometimes include people.

NOTE 2 This is the definition given in ISO/IEC 2382-14-01-01.

3.2.29
hardware safety integrity
part of the safety integrity of the safety instrumented function relating to random hardware failures in a dangerous mode of failure

NOTE 1 The term relates to failures in a dangerous mode. That is, those failures of a safety instrumented function that would impair its safety integrity. The two parameters that are relevant in this context are the overall dangerous failure rate and the probability of failure to operate on demand.

NOTE 2 See 3.2.86.

NOTE 3 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.30
harm
physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment

NOTE This definition matches ISO/IEC Guide 51.

3.2.31
hazard
potential source of harm

NOTE 1 This definition (without notes) matches 3.4 of ISO/IEC Guide 51.

NOTE 2 The term includes danger to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

3.2.32
human error
mistake
human action or inaction that produces an unintended result

NOTE This is the definition found in ISO/IEC 2382-14-02-03 and differs from that given in IEV 191-05-25 by the addition of “or inaction”.

3.2.33
analyse d'impact
activité consistant à déterminer l'effet que la modification à une fonction ou à un composant d'un système a sur les autres fonctions ou les autres composants de ce système tout comme sur d'autres systèmes

3.2.34
département indépendant
département distinct et séparé de ceux responsables des activités qui se déroulent lors des phases spécifiques du cycle de vie de sécurité et qui est chargé de l'évaluation de la sécurité fonctionnelle ou de la validation

3.2.35
organisation indépendante
organisation distincte et séparée, par sa direction et ses autres ressources, de celles responsables des activités qui se déroulent lors des phases spécifiques du cycle de vie de sécurité et qui est chargée de l'évaluation de la sécurité fonctionnelle ou de la validation

3.2.36
personne indépendante
personne distincte et séparée de celles responsables des activités qui se déroulent lors des phases du cycle de vie de sécurité, qui est chargée de l'évaluation de la sécurité fonctionnelle ou de la validation, et qui n'a pas de responsabilité directe dans ces activités

3.2.37
fonction d'entrée
fonction qui contrôle le processus et ses équipements associés afin de fournir des informations d'entrée à l'unité logique

NOTE Une fonction d'entrée peut être une fonction manuelle.

3.2.38
instrument
appareil, utilisé pour effectuer une action (généralement présent dans les systèmes instrumentés)

NOTE Les systèmes instrumentés dans le domaine des processus se composent généralement de capteurs (par exemple, de pression, de débit, de température), d'unités logiques ou de systèmes de commande (par exemple, automates programmables, systèmes de commande répartis), et d'éléments terminaux (par exemple, vannes de commande). Dans des cas particuliers, les systèmes instrumentés peuvent être des systèmes instrumentés de sécurité (voir 3.2.72).

3.2.39
fonction logique
fonction qui réalise les transformations entre les informations d'entrée (fournies par une ou plusieurs fonctions d'entrée) et les informations de sortie (utilisées par une ou plusieurs fonctions de sortie); les fonctions logiques assurent la transformation d'une ou de plusieurs fonctions d'entrée en une ou plusieurs fonctions de sortie

NOTE Pour d'autres directives voir la CEI 61131-3 et la CEI 60617-12.

3.2.40
unité logique
partie d'un BPCS ou d'un SIS qui exécute une ou plusieurs fonctions logiques.

NOTE 1 Dans la CEI 61511, les termes suivants sont utilisés pour des systèmes logiques:

– systèmes logiques électriques pour la technologie électromécanique;

– systèmes logiques électroniques pour la technologie électronique;

– systèmes logiques programmables pour les systèmes électroniques programmables.

NOTE 2 Des exemples sont: systèmes électriques, systèmes électroniques, systèmes électroniques programmables, systèmes pneumatiques, systèmes hydrauliques. Les capteurs et les éléments terminaux ne font pas partie de l'unité logique.

3.2.33
impact analysis
activity of determining the effect that a change to a function or component will have to other functions or components in that system as well as to other systems

3.2.34
independent department
department which is separate and distinct from the departments responsible for the activities which take place during the specific phase of the safety life cycle that is subject to the functional safety assessment or validation

3.2.35
independent organization
organization which is separate and distinct, by management and other resources, from the organizations responsible for the activities which take place during the specific phase of the safety life cycle that is subject to the functional safety assessment or validation

3.2.36
independent person
person who is separate and distinct from the activities which take place during the specific phase of the safety life cycle that is subject to the functional safety assessment or validation and does not have direct responsibility for those activities

3.2.37
input function
function which monitors the process and its associated equipment in order to provide input information for the logic solver

NOTE An input function could be a manual function.

3.2.38
instrument
apparatus used in performing an action (typically found in instrumented systems)

NOTE Instrumented systems in the process sector are typically composed of sensors (for example, pressure, flow, temperature transmitters), logic solvers or control systems (for example, programmable controllers, distributed control systems), and final elements (for example, control valves). In special cases, instrumented systems can be safety instrumented systems (see 3.2.72).

3.2.39
logic function
function which performs the transformations between input information (provided by one or more input functions) and output information (used by one or more output functions); logic functions provide the transformation from one or more input functions to one or more output functions

NOTE For further guidance, see IEC 61131-3 and IEC 60617-12.

3.2.40
logic solver
that portion of either a BPCS or SIS that performs one or more logic function(s)

NOTE 1 In IEC 61511 the following terms for logic systems are used:

– electrical logic systems for electro-mechanical technology;

– electronic logic systems for electronic technology;

– PE logic system for programmable electronic systems.

NOTE 2 Examples are: electrical systems, electronic systems, programmable electronic systems, pneumatic systems, hydraulic systems. Sensors and final elements are not part of the logic solver.

3.2.40.1
unité logique configurée pour la sécurité
unité logique de catégorie «électronique programmable pour usage général industriel», spécifiquement configurée pour être utilisée dans des applications de sécurité, en accord avec 11.5

3.2.41
interface de maintenance/d'ingénierie
l'interface de maintenance/d'ingénierie est constituée des matériels et des logiciels fournis, afin de permettre la maintenance ou la modification ad hoc du SIS. Elle peut comprendre des instructions et des diagnostics, pouvant être trouvés dans le logiciel, les terminaux de programmation avec les protocoles de transmission appropriés, des outils de diagnostic, des indicateurs, des dispositifs de dérivation, des dispositifs d'essai, et des dispositifs d'étalonnage

3.2.42
atténuation
action qui atténue la (les) conséquence(s) d'un événement dangereux

NOTE On peut donner comme exemple la dépressurisation de secours lors d'une détection d'un feu confirmé ou d'une fuite de gaz.

3.2.43
mode de fonctionnement
la manière dont fonctionne une fonction instrumentée de sécurité

3.2.43.1
fonction instrumentée de sécurité en mode sollicitation
lorsqu'une action spécifiée (par exemple, fermeture d'une vanne) est effectuée en réponse aux conditions du processus ou à d'autres sollicitations. Dans l'éventualité d'une défaillance dangereuse de la fonction instrumentée de sécurité, un danger potentiel n'apparaît qu'en cas de défaillance dans le processus ou dans le BPCS

3.2.43.2
fonction instrumentée de sécurité en mode continu
lorsqu'en cas de défaillance dangereuse de la fonction instrumentée de sécurité, un danger potentiel apparaît, sans autre défaillance, sauf si une action est entreprise pour le prévenir

NOTE 1 Le mode continu couvre les fonctions instrumentées de sécurité qui mettent en oeuvre une commande continue pour maintenir la sécurité fonctionnelle.

NOTE 2 Dans les applications en mode sollicitation où le taux de demande est plus fréquent qu'une fois par an, le taux de danger ne sera pas supérieur au taux des défaillances dangereuses de la fonction instrumentée de sécurité. Dans ce cas, il conviendra normalement d'utiliser les critères du mode continu.

NOTE 3 Les mesures cibles de défaillances pour les fonctions instrumentées de sécurité fonctionnant en mode sollicitation et en mode continu sont définies dans les Tableaux 3 et 4.

NOTE 4 Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.44
module
ensemble monobloc de composants de matériel exécutant une fonction matérielle spécifique (c'est-à-dire, module d'entrée numérique, module de sortie analogique), ou programme d'application réutilisable (peut être interne à un programme ou un ensemble de programmes) et qui supporte une fonction spécifique. Par exemple: partie d'un programme machine remplissant une fonction spécifique

NOTE 1 Dans le contexte de la CEI 61131-3, un module logiciel est une fonction ou un bloc de fonctions.

NOTE 2 Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans le domaine des processus.

3.2.40.1
safety configured logic solver
general purpose industrial grade PE logic solver which is specifically configured for use in safety applications in accordance with 11.5

3.2.41
maintenance/engineering interface
maintenance/engineering interface is that hardware and software provided to allow proper SIS maintenance or modification. It can include instructions and diagnostics which may be found in software, programming terminals with appropriate communication protocols, diagnostic tools, indicators, bypass devices, test devices, and calibration devices

3.2.42
mitigation
action that reduces the consequence(s) of a hazardous event

NOTE Examples include emergency depressurization on detection of confirmed fire or gas leak.

3.2.43
mode of operation
way in which a safety instrumented function operates

3.2.43.1
demand mode safety instrumented function
where a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS

3.2.43.2
continuous mode safety instrumented function
where in the event of a dangerous failure of the safety instrumented function a potential hazard will occur without further failure unless action is taken to prevent it

NOTE 1 Continuous mode covers those safety instrumented functions which implement continuous control to maintain functional safety.

NOTE 2 In demand mode applications where the demand rate is more frequent than once per year, the hazard rate will not be higher than the dangerous failure rate of the safety instrumented function. In such a case, it will normally be appropriate to use the continuous mode criteria.

NOTE 3 The target failure measures for safety instrumented functions operating in demand mode and continuous mode are defined in Tables 3 and 4.

NOTE 4 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.44
module
self-contained assembly of hardware components that performs a specific hardware function (i.e., digital input module, analogue output module), or reusable application program (can be internal to a program or a set of programs) that support a specific function, for example, portion of a computer program that carries out a specific function

NOTE 1 In the context of IEC 61131-3, a software module is a function or function block.

NOTE 2 This term deviates from the definition in IEC 61508-4 to reflect differences in the process sector.

3.2.45
MooN
système instrumenté de sécurité, ou partie de celui-ci, composé de «**N**» canaux indépendants, qui sont connectés de telle manière que «**M**» canaux sont suffisants pour exécuter la fonction instrumentée de sécurité

3.2.46
réduction de risque nécessaire
réduction de risque requise pour assurer que le risque est réduit à un niveau tolérable

3.2.47
système non programmable (NP)
système basé sur des technologies ne mettant pas en œuvre un ordinateur (c'est-à-dire, un système non basé sur une électronique programmable [PE] ou sur un logiciel)

NOTE Des exemples pourraient être les systèmes électriques ou électroniques câblés, les systèmes mécaniques, hydrauliques, ou pneumatiques.

3.2.48
interface opérateur
les moyens par lesquels les informations sont communiquées entre un opérateur humain et le SIS (par exemple, écrans cathodiques, voyants lumineux, boutons-poussoir, klaxons, alarmes); l'interface opérateur est parfois désignée sous le nom d'interface homme-machine (IHM ou HMI)

3.2.49
systèmes relatifs à la sécurité basés sur une autre technologie
systèmes relatifs à la sécurité basés sur une technologie autre qu'électrique, électronique ou électronique programmable

NOTE Une soupape de sécurité est un «système relatif à la sécurité basé sur une autre technologie». Les «systèmes relatifs à la sécurité basés sur une autre technologie» peuvent inclure les systèmes hydrauliques et pneumatiques.

3.2.50
fonction de sortie
fonction qui commande le processus et ses équipements associés, en fonction des informations de l'actionneur terminal, à partir de la fonction logique

3.2.51
phase
période comprise dans le cycle de vie de sécurité, où sont mises en œuvre les activités décrites dans cette norme

3.2.52
prévention
action qui réduit la probabilité d'occurrence d'un événement dangereux

3.2.53
utilisation antérieure
voir «validé en utilisation» (3.2.60)

3.2.54
risque de processus
risque provenant des conditions du processus provoquées par des événements anormaux (comprenant un mauvais fonctionnement du BPCS)

NOTE 1 Dans ce contexte, il s'agit du risque associé à l'événement dangereux spécifique pour lequel les SIS doivent être utilisés afin d'apporter la réduction de risque nécessaire (c'est-à-dire le risque associé à la sécurité fonctionnelle).

3.2.45
MooN
safety instrumented system, or part thereof, made up of "**N**" independent channels, which are so connected, that "**M**" channels are sufficient to perform the safety instrumented function

3.2.46
necessary risk reduction
risk reduction required to ensure that the risk is reduced to a tolerable level

3.2.47
non-programmable (NP) system
system based on non-computer technologies (i.e., a system not based on programmable electronics [PE] or software)

NOTE Examples would include hard-wired electrical or electronic systems, mechanical, hydraulic, or pneumatic systems.

3.2.48
operator interface
means by which information is communicated between a human operator(s) and the SIS (for example, CRTs, indicating lights, push-buttons, horns, alarms); the operator interface is sometimes referred to as the human-machine interface (HMI)

3.2.49
other technology safety related systems
safety related systems that are based on a technology other than electrical, electronic, or programmable electronic

NOTE A relief valve is "another technology safety related system". "Other technology safety related systems" may include hydraulic and pneumatic systems.

3.2.50
output function
function which controls the process and its associated equipment according to final actuator information from the logic function

3.2.51
phase
period within the safety life cycle where activities described in this standard take place

3.2.52
prevention
action that reduces the frequency of occurrence of a hazardous event

3.2.53
prior use
see "proven-in-use" (see 3.2.60)

3.2.54
process risk
risk arising from the process conditions caused by abnormal events (including BPCS malfunction)

NOTE 1 The risk in this context is that associated with the specific hazardous event in which SIS are to be used to provide the necessary risk reduction (i.e., the risk associated with functional safety).

NOTE 2 L'analyse de risque de processus est décrite dans la CEI 61511-3. L'objectif principal dans la détermination du risque de processus est d'établir un point de référence pour le risque, sans prendre en compte les couches de protection.

NOTE 3 Il convient que l'évaluation de ce risque comprenne les problèmes associés aux facteurs humains.

NOTE 4 Ce terme équivaut au «risque EUC» de la CEI 61508-4.

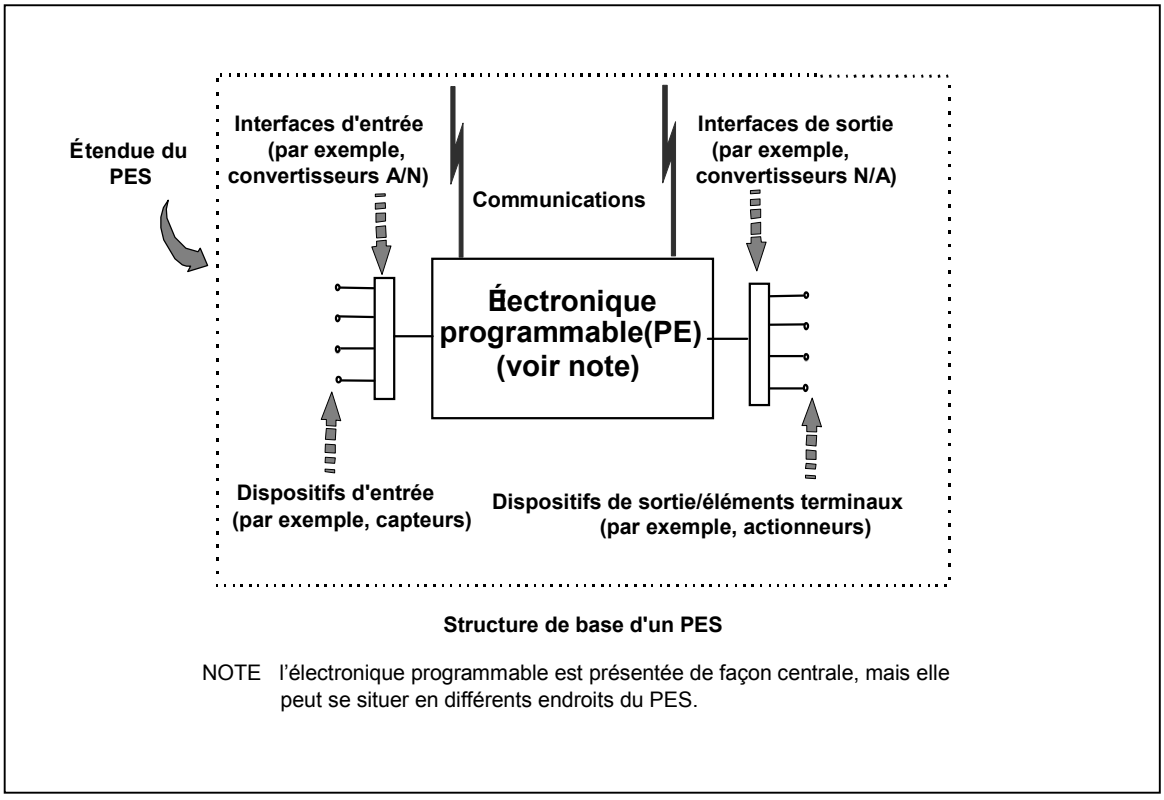
3.2.55
électronique programmable (PE)
composant électronique ou dispositif faisant partie d'un PES et basé sur les technologies de l'informatique. Le terme englobe à la fois le matériel et le logiciel, et les unités d'entrée et de sortie

NOTE 1 Ce terme recouvre les appareils micro-électroniques basés sur une ou plusieurs unités centrales de traitement (CPU) associées à des mémoires. Des exemples de dispositifs électroniques programmables dans le domaine des processus comprennent:

– capteurs intelligents et éléments terminaux;
– unités logiques électroniques programmables comprenant:
  – contrôleurs programmables;
  – automates programmables;
  – contrôleurs de boucle.

NOTE 2 Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.56
système électronique programmable (PES)
système de commande, de protection ou de surveillance basé sur un ou plusieurs dispositifs électroniques programmables, comprenant tous les éléments du système, tels que les alimentations, les capteurs et d'autres dispositifs d'entrée, en passant par les autoroutes de données et d'autres voies de communication, jusqu'aux actionneurs et d'autres dispositifs de sortie (voir la Figure 6)



IEC 3245/02

Figure 6 – Système électronique programmable (PES): structure et terminologie

NOTE 2 Process risk analysis is described in IEC 61511-3. The main purpose of determining the process risk is to establish a reference point for the risk without taking into account the protection layers.

NOTE 3 Assessment of this risk should include associated human factor issues.

NOTE 4 This term equates to “EUC risk” in IEC 61508-4.

3.2.55
programmable electronics (PE)
electronic component or device forming part of a PES and based on computer technology. The term encompasses both hardware and software and input and output units

NOTE 1 This term covers micro-electronic devices based on one or more central processing units (CPU) together with associated memories. Examples of process sector programmable electronics include

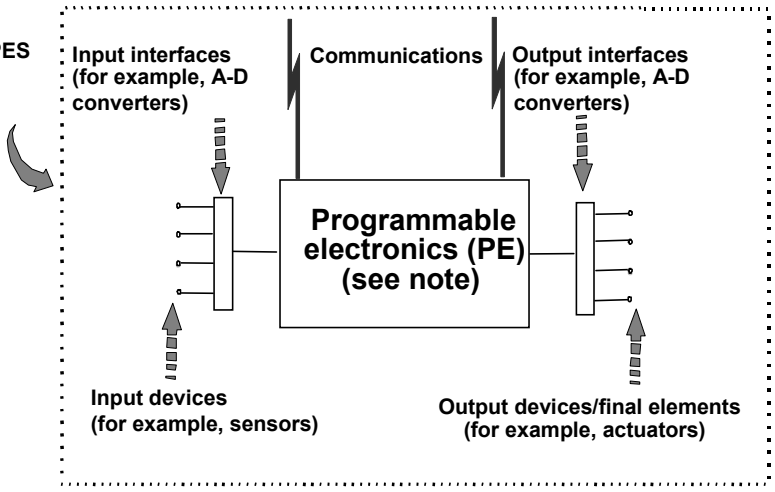
– smart sensors and final elements;

– programmable electronic logic solvers including

- programmable controllers;
- programmable logic controllers.
- loop controllers.

NOTE 2 This term differs from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.56
programmable electronic system (PES)
system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, actuators and other output devices (see Figure 6)



Basic PES structure

NOTE The programmable electronics are shown centrally located but could exist at several places in the PES.

IEC 3245/02

Figure 6 – Programmable electronic system (PES): structure and terminology

3.2.57
programmation
processus consistant à concevoir, à écrire et à tester un ensemble d'instructions pour résoudre un problème ou traiter des données

NOTE Dans cette norme la programmation est typiquement associée à une électronique programmable (PE).

3.2.58
test périodique
essai effectué pour révéler des défauts non détectés dans un système instrumenté de sécurité, de telle sorte que, au besoin, le système puisse être restauré dans sa fonctionnalité de conception

3.2.59
couche de protection
tout mécanisme indépendant réduisant le risque par commande, prévention ou atténuation

NOTE Cela peut être un mécanisme d'ingénierie de processus, tel que la taille des cuves contenant des produits chimiques dangereux, un mécanisme de génie mécanique, tel qu'une soupape de sécurité, un système instrumenté de sécurité ou une procédure administrative, tel qu'un plan de secours contre un danger imminent. Ces réponses peuvent être automatisées ou initiées par des actions humaines (voir la Figure 9).

3.2.60
validé en utilisation
un composant peut être considéré comme «validé en utilisation» lorsqu'une évaluation documentée a apporté des preuves, basées sur l'utilisation antérieure du composant, que ce dernier convient à l'utilisation dans un système instrumenté de sécurité (voir «utilisation antérieure» en 11.5).

NOTE Ce terme diffère de la CEI 61508 pour refléter les différences dans la technologie du domaine des processus.

3.2.61
qualité
ensemble des caractéristiques d'une entité qui portent sur sa capacité à satisfaire aux besoins exprimés et implicites

NOTE Voir l'ISO 9000 pour plus de détails.

3.2.62
défaillances aléatoires du matériel
défaillances survenant de manière aléatoire et résultant de divers mécanismes de dégradation au sein du matériel

NOTE 1 Il existe plusieurs mécanismes de dégradation se produisant à des probabilités différentes dans divers composants et, puisque les tolérances de fabrication ont pour conséquence une défaillance des composants provoquée par ces mécanismes après des durées de fonctionnement diverses, les défaillances survenant dans l'ensemble des équipements comprenant plusieurs composants, surviennent à des probabilités prévisibles, mais à des instants imprévisibles (car aléatoires).

NOTE 2 L'une des différences majeures entre les défaillances aléatoires du matériel et les défaillances systématiques (voir 3.2.85) est que les taux de défaillance du système (ou toute autre mesure appropriée), engendrés par les défaillances aléatoires du matériel, peuvent être prédits, alors que les défaillances systématiques, de par leur nature même, ne peuvent être prédites. C'est-à-dire que les taux de défaillance du système, issus des défaillances aléatoires du matériel, peuvent être quantifiés, mais que ceux issus des défaillances systématiques ne peuvent pas l'être de manière statistique, du fait que les événements y conduisant ne peuvent pas facilement être prédits.

3.2.63
redondance
utilisation de plusieurs éléments ou systèmes pour exécuter la même fonction; la redondance peut être mise en œuvre par des éléments identiques (redondance identique) ou par des éléments différents (redondance diverse)

NOTE 1 Des exemples en sont l'utilisation de composants fonctionnels en double et l'adjonction de bits de parité.

NOTE 2 La redondance sert essentiellement à améliorer la fiabilité ou la disponibilité.

3.2.57
programming
process of designing, writing and testing a set of instructions for solving a problem or processing data

NOTE In this standard, programming is typically associated with PE.

3.2.58
proof test
test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality

3.2.59
protection layer
any independent mechanism that reduces risk by control, prevention or mitigation

NOTE It could be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical engineering mechanism such as a relief valve, a safety instrumented system or an administrative procedure such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions (see Figure 9).

3.2.60
proven-in-use
when a documented assessment has shown that there is appropriate evidence, based on the previous use of the component, that the component is suitable for use in a safety instrumented system (see “prior use” in 11.5)

NOTE This term deviates from IEC 61508 to reflect differences in process sector technology.

3.2.61
quality
totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs

NOTE See ISO 9000 for more details.

3.2.62
random hardware failure
failure, occurring at a random time, which results from a variety of degradation mechanisms in the hardware

NOTE 1 There are many degradation mechanisms occurring at different rates in different components and since manufacturing tolerances cause components to fail due to these mechanisms after different times in operation, failures of a total equipment comprising many components occur at predictable rates but at unpredictable (i.e., random) times.

NOTE 2 A major distinguishing feature between random hardware failures and systematic failures (see 3.2.85) is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted but systematic failures, by their very nature, cannot be predicted. That is, system failure rates arising from random hardware failures can be quantified but those arising from systematic failures cannot be statistically quantified because the events leading to them cannot easily be predicted.

3.2.63
redundancy
use of multiple elements or systems to perform the same function; redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy)

NOTE 1 Examples are the use of duplicate functional components and the addition of parity bits.

NOTE 2 Redundancy is used primarily to improve reliability or availability.

NOTE 3 La définition du VEI 191-15-01 est moins complète [ISO/CEI 2382-14-01-11].

NOTE 4 Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.64
risque
combinaison de la probabilité d'occurrence d'un dommage et de la gravité de ce dernier

NOTE Pour plus de commentaires sur ce concept, voir l'Article 8.

3.2.65
défaillance en sécurité
défaillance qui n'a pas la potentialité de mettre le système instrumenté de sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction

NOTE 1 Le fait que cette potentialité se réalise ou non peut dépendre de l'architecture du canal du système.

NOTE 2 D'autres noms utilisés pour «défaillance en sécurité» sont: défaillance intempestive, déclenchement parasite de défaillance, faux déclenchement de défaillance ou défaillance hors sécurité.

3.2.65.1
proportion de défaillances en sécurité
proportion du taux global des défaillances aléatoires de matériel d'un dispositif qui a comme conséquence une défaillance en sécurité ou une défaillance dangereuse détectée

3.2.66
état de sécurité
état du processus lorsque la sécurité est réalisée

NOTE 1 Durant son évolution depuis un état potentiellement dangereux vers un état de sécurité final, le processus est susceptible de passer par un certain nombre d'états de sécurité intermédiaires. Dans certaines situations, l'état de sécurité n'existe que durant le laps de temps où le processus est continuellement commandé. Cette commande continue peut s'étendre sur une période de temps courte ou indéfinie.

NOTE 2 Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.67
sécurité
absence de risque inacceptable

NOTE Cette définition correspond au Guide ISO/CEI 51.

3.2.68
fonction de sécurité
fonction à réaliser par un système SIS, par un système relatif à la sécurité basé sur une autre technologie, ou par des dispositifs externes de réduction de risque, prévue pour assurer ou maintenir un état de sécurité au processus, par rapport à un événement dangereux spécifique

NOTE Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.69
fonction de commande instrumentée de sécurité
fonction instrumentée de sécurité avec un SIL spécifié, fonctionnant en mode continu, qui est nécessaire pour prévenir l'apparition d'un état dangereux et/ou pour atténuer ses conséquences

3.2.70
système de commande instrumenté de sécurité
système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions de commande instrumentées de sécurité

NOTE Les systèmes de commande instrumentés de sécurité sont rares dans les industries de processus. Dans l'éventualité où de tels systèmes sont identifiés, ils devront être traités comme des cas particuliers et être conçus au cas par cas. Il convient que les exigences de cette norme s'appliquent, mais une analyse détaillée plus approfondie peut être exigée pour démontrer que le système est capable d'atteindre les exigences de sécurité.

NOTE 3 The definition in IEV 191-15-01 is less complete [ISO/IEC 2382-14-01-11].

NOTE 4 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.64
risk
combination of the frequency of occurrence of harm and the severity of that harm

NOTE For more discussion on this concept, see Clause 8.

3.2.65
safe failure
failure which does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state

NOTE 1 Whether or not the potential is realized may depend on the channel architecture of the system.

NOTE 2 Other names used for safe failure are nuisance failure, spurious trip failure, false trip failure or fail-to-safe failure.

3.2.65.1
safe failure fraction
fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure

3.2.66
safe state
state of the process when safety is achieved

NOTE 1 In going from a potentially hazardous condition to the final safe state, the process may have to go through a number of intermediate safe-states. For some situations, a safe state exists only so long as the process is continuously controlled. Such continuous control may be for a short or an indefinite period of time.

NOTE 2 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.67
safety
freedom from unacceptable risk

NOTE This definition is according to ISO/IEC Guide 51.

3.2.68
safety function
function to be implemented by an SIS, other technology safety related system or external risk, reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event

NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.69
safety instrumented control function
safety instrumented function with a specified SIL operating in continuous mode which is necessary to prevent a hazardous condition from arising and/or to mitigate its consequences

3.2.70
safety instrumented control system
instrumented system used to implement one or more safety instrumented control functions

NOTE Safety instrumented control systems are rare within the process industries. Where such systems are identified, they will need to be treated as a special case and designed on an individual basis. The requirements within this standard should apply but further detailed analysis may be required to demonstrate that the system is capable of achieving the safety requirements.

3.2.71
fonction instrumentée de sécurité (SIF)
fonction de sécurité avec un niveau d'intégrité de sécurité spécifié, nécessaire pour atteindre la sécurité fonctionnelle. Une fonction instrumentée de sécurité peut être, soit une fonction de protection instrumentée de sécurité, soit une fonction de commande instrumentée de sécurité

3.2.72
système instrumenté de sécurité (SIS)
système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unité(s) logique(s) et d'élément(s) terminal(aux) (par exemple, voir la Figure 7)

NOTE 1 Celui-ci peut inclure, soit des fonctions de commande instrumentées de sécurité, soit des fonctions de protection instrumentées de sécurité, ou les deux.

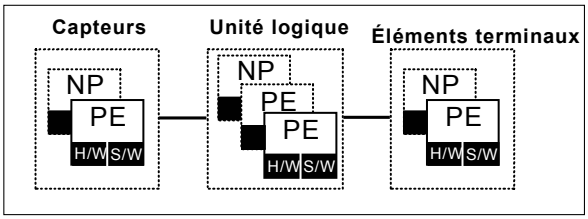
NOTE 2 Il convient que les constructeurs et les fournisseurs de dispositifs SIS se reportent à l'Article 1, points a) à d).

NOTE 3 Un SIS peut ou peut ne pas inclure le logiciel.

NOTE 4 Voir Article A.2.

NOTE 5 Lorsqu'une action humaine fait partie d'un SIS, la disponibilité et la fiabilité de l'action de l'opérateur doivent être spécifiées dans le SRS et être incluses dans les calculs de performances du SIS. Voir la CEI 61511-2 pour prendre connaissance des directives sur la façon d'inclure la disponibilité et la fiabilité de l'opérateur dans les calculs du SIL.

Architecture SIS et exemple de fonction instrumentée de sécurité avec différents dispositifs



IEC 3246/02

Figure 7 – Exemple d'architecture SIS

3.2.73
intégrité de sécurité
probabilité moyenne pour qu'un système instrumenté de sécurité exécute de manière satisfaisante les fonctions instrumentées de sécurité requises, dans toutes les conditions spécifiées et dans une période de temps spécifiée

NOTE 1 Plus le niveau d'intégrité de sécurité de la fonction instrumentée sécurité (SIF) est élevé, plus la probabilité d'une défaillance de la SIF dans l'exécution des fonctions instrumentées de sécurité requises, est faible.

NOTE 2 Il y a quatre niveaux d'intégrité de sécurité pour les fonctions instrumentées de sécurité.

NOTE 3 Il convient que l'évaluation de l'intégrité de sécurité prenne en compte toutes les causes de défaillance (à la fois les défaillances aléatoires du matériel et les défaillances systématiques) conduisant à un état de non-sécurité, par exemple les défaillances de matériel, les défaillances induites du logiciel et les défaillances dues aux perturbations électriques. Certaines de ces défaillances, en particulier les défaillances aléatoires du matériel, peuvent être quantifiées à l'aide de mesures telles que celle du taux de défaillance en mode de défaillance dangereux, ou de la probabilité de défaillance de fonctionnement à la sollicitation d'une fonction instrumentée de sécurité. Cependant, l'intégrité de sécurité d'une SIF dépend également de plusieurs facteurs, qui ne peuvent être précisément quantifiés, mais simplement considérés d'un point de vue qualitatif.

NOTE 4 L'intégrité de sécurité comprend l'intégrité de sécurité du matériel et l'intégrité de sécurité systématique.

3.2.74
niveau d'intégrité de sécurité (SIL)
niveau discret (parmi quatre possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions instrumentées de sécurité, à allouer aux systèmes instrumentés de sécurité. Le niveau d'intégrité de sécurité 4 possède le plus haut degré d'intégrité; le niveau 1 possède le plus bas

NOTE 1 Les mesures cibles de défaillances pour les niveaux d'intégrité de sécurité sont indiquées dans les Tableaux 3 et 4.

3.2.71
safety instrumented function (SIF)
safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function

3.2.72
safety instrumented system (SIS)
instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s) (for example, see Figure 7)

NOTE 1 This can include either safety instrumented control functions or safety instrumented protection functions or both.

NOTE 2 Manufacturers and suppliers of SIS devices should refer to Clause 1 a) through d) inclusive.

NOTE 3 A SIS may or may not include software.

NOTE 4 See Clause A.2.

NOTE 5 When a human action is a part of an SIS, the availability and reliability of the operator action must be specified in the SRS and included in the performance calculations for the SIS. See IEC 61511-2 for guidance on how to include operator availability and reliability in SIL calculations.

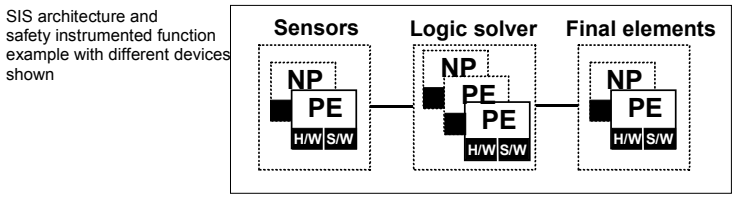


Figure 7 – Example of SIS architecture

3.2.73
safety integrity
average probability of a safety instrumented system satisfactorily performing the required safety instrumented functions under all the stated conditions within a stated period of time

NOTE 1 The higher the safety integrity level, the higher the probability that the required safety instrumented function (SIF) will be carried out.

NOTE 2 There are four levels of safety integrity for safety instrumented functions.

NOTE 3 In determining safety integrity, all causes of failures (both random hardware failures and systematic failures) which lead to an unsafe state should be included; for example, hardware failures, software induced failures and failures due to electrical interference. Some of these types of failure, in particular random hardware failures, may be quantified using such measures as the failure rate in the dangerous mode of failure or the probability of a safety instrumented function failing to operate on demand. However, the safety integrity of an SIF also depends on many factors, which cannot be accurately quantified but can only be considered qualitatively.

NOTE 4 Safety integrity comprises hardware safety integrity and systematic safety integrity.

3.2.74
safety integrity level (SIL)
discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest

NOTE 1 The target failure measures for the safety integrity levels are specified in Tables 3 and 4.

NOTE 2 Il est possible d'utiliser plusieurs systèmes de niveau d'intégrité de sécurité inférieurs pour satisfaire au besoin d'une fonction de niveau plus élevée (par exemple, en utilisant un système à la fois de SIL 2 et de SIL 1 pour satisfaire au besoin d'une fonction de SIL 3).

NOTE 3 Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.75
spécification des exigences concernant l'intégrité de sécurité
spécification qui contient les exigences concernant l'intégrité de sécurité des fonctions instrumentées de sécurité devant être exécutées par le(s) système(s) instrumenté(s) de sécurité

NOTE 1 Cette spécification constitue une partie (partie concernant l'intégrité de sécurité) de la spécification des exigences concernant la sécurité (voir 3.2.78).

NOTE 2 Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.76
cycle de vie de sécurité
activités nécessaires à la mise en œuvre de fonction(s) instrumentée(s) de sécurité, se déroulant au cours d'une période de temps, qui commence à la phase de conception d'un projet et se termine lorsque toutes les fonctions instrumentées de sécurité ne sont plus disponibles à l'utilisation

NOTE 1 Le terme «cycle de vie de sécurité fonctionnelle» est strictement plus précis, mais l'adjectif «fonctionnelle» n'est pas considéré comme étant nécessaire dans ce cas, c'est-à-dire dans le contexte de la présente norme.

NOTE 2 Le modèle de cycle de vie de sécurité utilisé dans la CEI 61511 est donné par la Figure 8.

3.2.77
manuel de sécurité
un manuel de sécurité définit comment le dispositif, le sous-système ou le système peuvent être appliqués sans risque

NOTE Celui-ci peut être un document autonome, un manuel didactique, un manuel de programmation, un document standard, ou inclus dans un (des) document(s) utilisateur définissant des limitations d'application.

3.2.78
spécification des exigences concernant la sécurité
spécification qui contient toutes les exigences des fonctions instrumentées de sécurité devant être exécutées par les systèmes instrumentés de sécurité

3.2.79
logiciel de sécurité
logiciel dans un système instrumenté de sécurité avec une fonctionnalité de logiciel d'application, intégré ou utilitaire

3.2.80
capteur
dispositif ou combinaison des dispositifs, qui mesurent l'état du processus (par exemple, transmetteurs, transducteurs, contacteurs de processus, contacteurs de position)

3.2.81
logiciel
création intellectuelle comprenant les programmes, les données, les procédures et règles, ainsi que toute documentation se référant au fonctionnement d'un système de traitement de données

NOTE 1 Le logiciel est indépendant du support sur lequel il a été enregistré.

NOTE 2 Cette définition, sans la note 1, diffère de l'ISO 2382-1, et la définition complète diffère de l'ISO 9000-3 par l'ajout du mot «données».

NOTE 2 It is possible to use several lower safety integrity level systems to satisfy the need for a higher level function (for example, using a SIL 2 and a SIL 1 system together to satisfy the need for a SIL 3 function).

NOTE 3 This term differs from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.75
safety integrity requirements specification
specification that contains the safety integrity requirements of the safety instrumented functions that have to be performed by the safety instrumented system(s)

NOTE 1 This specification is one part (the safety integrity part) of the safety requirements specification (see 3.2.78).

NOTE 2 This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.76
safety life cycle
necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use

NOTE 1 The term “functional safety life cycle” is strictly more accurate, but the adjective “functional” is not considered necessary in this case within the context of this standard.

NOTE 2 The safety life-cycle model used in IEC 61511 is shown in Figure 8.

3.2.77
safety manual
manual which defines how the device, subsystem or system can be safely applied

NOTE This could be a stand-alone document, an instructional manual, a programming manual, a standard document, or included in the user document(s) defining application limitations.

3.2.78
safety requirements specification
specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems

3.2.79
safety software
software in a safety instrumented system with application, embedded or utility software functionality

3.2.80
sensor
device or combination of devices, which measure the process condition (for example, transmitters, transducers, process switches, position switches)

3.2.81
software
intellectual creation comprising the programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system

NOTE 1 Software is independent of the medium on which it is recorded.

NOTE 2 This definition without note 1 differs from ISO 2382-1, and the full definition differs from ISO 9000-3 by the addition of the word data.

3.2.81.1
langages logiciel dans les sous-systèmes d'un SIS

3.2.81.1.1
langage de programme figé (FPL)
dans ce type de langage, l'utilisateur est limité à l'ajustement de quelques paramètres (par exemple, gamme d'un transmetteur de pression, seuils d'alarme, adresses de réseau)

NOTE Des exemples représentatifs de dispositifs avec FPL sont: capteur intelligent (par exemple, transmetteur de pression), vanne intelligente, séquence de contrôleur d'événements, boîte d'alarme intelligente, petits systèmes d'enregistrement de données.

3.2.81.1.2
langage de variabilité limitée (LVL)
ce type de langage est conçu pour être compréhensible par les utilisateurs du domaine des processus et fournit la possibilité de combiner des fonctions de bibliothèque, prédéfinies, spécifiques à une application, pour mettre en œuvre les spécifications des exigences concernant la sécurité. Un LVL fournit une correspondance fonctionnelle étroite avec les fonctions nécessaires pour réaliser l'application

NOTE 1 Des exemples typiques de LVL sont donnés dans la CEI 61131-3. Ils comprennent: le langage à contacts, le langage en blocs fonctionnels et le diagramme fonctionnel en séquence.

NOTE 2 Exemple typique des systèmes utilisant le LVL: un PLC standard (par exemple, automate programmable pour la gestion d'un brûleur).

3.2.81.1.3
langage de variabilité totale (FVL)
ce type de langage est conçu pour être compréhensible par les informaticiens (programmeurs), et fournit la possibilité de mettre en œuvre une gamme étendue de fonctions et d'applications

NOTE 1 Un exemple typique de système utilisant le FVL est l'ordinateur d'usage général.

NOTE 2 Dans le domaine des processus, le FVL se trouve dans les logiciels intégrés et rarement dans les logiciels d'application.

NOTE 3 Parmi les exemples de FVL on peut citer: l'Ada, le C, le Pascal, une liste d'instructions, les langages d'assemblage, le C++, le Java, le SQL.

3.2.81.2
type de programme logiciel

3.2.81.2.1
logiciel d'application
logiciel spécifique à l'application utilisateur. En général, il contient des séquences logiques, des acquittements, des termes et des expressions logiques qui contrôlent l'entrée, la sortie, les calculs appropriés, les décisions nécessaires pour satisfaire aux exigences fonctionnelles instrumentées de sécurité. Voir le langage figé et le langage de variabilité limitée

3.2.81.2.2
logiciel intégré
logiciel qui fait partie du système fourni par le constructeur et qui n'est pas accessible pour des modifications par l'utilisateur final. Le logiciel intégré est également désigné sous le nom de micro-logiciel ou de logiciel système. Voir 3.2.81.1.3, langage de variabilité totale

3.2.81.2.3
logiciel utilitaire
outils logiciels pour la création, la modification et la documentation des programmes d'application. Ces outils logiciels ne sont pas nécessaires pour l'exploitation du SIS

3.2.81.1
software languages in SIS subsystems

3.2.81.1.1
fixed program language (FPL)
in this type of language, the user is limited to adjustment of a few parameters (for example, range of the pressure transmitter, alarm levels, network addresses).

NOTE Typical examples of devices with FPL are: smart sensor (for example, pressure transmitter), smart valve, sequence of events controller, dedicated smart alarm box, small data logging systems.

3.2.81.1.2
limited variability language (LVL)
this type of language is designed to be comprehensible to process sector users, and provides the capability to combine predefined, application specific, library functions to implement the safety requirements specifications. An LVL provides a close functional correspondence with the functions required to achieve the application.

NOTE 1 Typical examples of LVL are given in IEC 61131-3. They include ladder diagram, function block diagram and sequential function chart.

NOTE 2 Typical example of systems using LVL: standard PLC (for example, programmable logic controller for burner management).

3.2.81.1.3
full variability language (FVL)
this type of language is designed to be comprehensible to computer programmers and provides the capability to implement a wide variety of functions and applications

NOTE 1 Typical example of systems using FVL are general purpose computers.

NOTE 2 In the process sector, FVL is found in embedded software and rarely in application software.

NOTE 3 FVL examples include: Ada, C, Pascal, Instruction List, assembler languages, C++, Java, SQL.

3.2.81.2
software program type

3.2.81.2.1
application software
software specific to the user application. In general, it contains logic sequences, permissives, limits and expressions that control the appropriate input, output, calculations, decisions necessary to meet the safety instrumented functional requirements. See fixed and limited variability language

3.2.81.2.2
embedded software
software that is part of the system supplied by the manufacturer and is not accessible for modification by the end-user. Embedded software is also referred to as firmware or system software. See 3.2.81.1.3, full variability language

3.2.81.2.3
utility software
software tools for the creation, modification, and documentation of application programs. These software tools are not required for the operation of the SIS

3.2.82
cycle de vie du logiciel
activités se déroulant au cours d'une période de temps allant de la phase pendant laquelle le logiciel est conçu jusqu'au moment où le logiciel n'est définitivement plus utilisé

NOTE 1 Le cycle de vie du logiciel inclut, typiquement, une phase de prescription, une phase de développement, une phase d'essai, une phase d'intégration, une phase d'installation et une phase de modification.

NOTE 2 Le logiciel ne peut pas être maintenu, mais il est modifiable.

3.2.83
sous-système
voir «système»

3.2.84
système
ensemble d'éléments qui interagissent selon un modèle précis; un élément d'un système peut être un autre système, appelé sous-système, ce dernier pouvant être lui-même, soit un système de commande, soit un système commandé, et peut être composé de matériel, de logiciel et comprendre des interactions avec l'être humain

NOTE 1 Une personne peut faire partie d'un système.

NOTE 2 Cette définition est différente de celle du VEI 351-01-01.

NOTE 3 Un système inclut des capteurs, des unités logiques, des éléments terminaux, des équipements de communication et auxiliaires appartenant au SIS (par exemple, câbles, tuyauterie, alimentation en énergie).

3.2.85
défaillance systématique
défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

NOTE 1 La maintenance corrective sans modification n'élimine pas, habituellement, la cause de la défaillance.

NOTE 2 Une défaillance systématique peut être induite en simulant la cause de la défaillance.

NOTE 3 Cette définition (jusqu'à la note 2) correspond à celle du VEI 191-04-19.

NOTE 4 Exemples des causes systématiques de défaillance comprenant l'erreur humaine dans:

– la spécification des exigences concernant la sécurité;

– la conception, la fabrication, l'installation et l'exploitation du matériel;

– la conception et/ou la mise en œuvre du logiciel.

3.2.86
intégrité de sécurité systématique
partie de l'intégrité de sécurité des fonctions instrumentées de sécurité qui se rapporte aux défaillances systématiques (voir la note 3 de 3.2.73) dans un mode de défaillance dangereux

NOTE 1 L'intégrité de sécurité systématique ne peut normalement pas être quantifiée (à la différence de l'intégrité de sécurité du matériel).

NOTE 2 Voir aussi 3.2.29.

3.2.87
niveau objectif de défaillances
probabilité prévisionnelle d'un mode de défaillance dangereux, à atteindre en fonction des exigences concernant l'intégrité de sécurité, spécifiée en termes: soit de probabilité moyenne de défaillance, lorsque les fonctions pour lesquelles le système a été conçu sont exécutées lorsqu'elles sont requises (en mode de fonctionnement en sollicitation), soit de probabilité d'une défaillance dangereuse, par heure, lors de l'exécution de la SIF (pour un mode de fonctionnement en continu)

NOTE Les valeurs numériques des mesures de défaillance cibles sont données par les Tableaux 3 et 4.

3.2.82
software life cycle
activities occurring during a period of time that starts when software is conceived and ends when the software is permanently disused

NOTE 1 A software life cycle typically includes a requirements phase, development phase, test phase, integration phase, installation phase and modification phase.

NOTE 2 Software cannot be maintained; rather, it is modified.

3.2.83
subsystem
see "system"

3.2.84
system
set of elements, which interact according to a design; an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction

NOTE 1 A person can be part of a system.

NOTE 2 This definition differs from IEV 351-01-01.

NOTE 3 A system includes the sensors, the logic solvers, final elements, communication and ancillary equipment belonging to SIS (for example, cables, tubing, power supply).

3.2.85
systematic failure
failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

NOTE 1 Corrective maintenance without modification would usually not eliminate the failure cause.

NOTE 2 A systematic failure can be induced by simulating the failure cause.

NOTE 3 This definition (up to note 2) matches IEV 191-04-19.

NOTE 4 Examples of systematic failure causes including human error in

– the safety requirements specification;

– the design, manufacture, installation and operation of the hardware;

– the design and/or implementation of the software.

3.2.86
systematic safety integrity
that part of the safety integrity of safety instrumented function relating to systematic failures (see note 3 of 3.2.73) in a dangerous mode of failure

NOTE 1 Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity).

NOTE 2 See also 3.2.29.

3.2.87
target failure measure
intended probability of dangerous mode failures to be achieved in respect of the safety integrity requirements, specified in terms of either the average probability of failure to perform the design function on demand (for a demand mode of operation) or the frequency of a dangerous failure to perform the SIF per hour (for a continuous mode of operation)

NOTE The numerical values for the target failure measures are given in Tables 3 and 4.

3.2.88
modèle
modèle logiciel
partie non spécifique et structurée de logiciel d'application qui peut être facilement changée pour supporter des fonctions spécifiques, tout en conservant la structure originale; par exemple, un modèle interactif d'écran contrôle l'enchaînement des écrans de l'application, mais n'est pas spécifique aux données qui sont présentées; un programmeur peut prendre le modèle générique et faire des modifications spécifiques de fonctions pour produire un nouvel écran destiné aux utilisateurs

NOTE Le terme connexe «modèle logiciel» est parfois utilisé. Typiquement, il se rapporte à un algorithme ou à un ensemble d'algorithmes qui ont été programmés pour exécuter une fonction ou un ensemble de fonctions souhaitées, et il est construit de telle sorte qu'il peut être utilisé dans de nombreux cas différents. Dans le contexte de la CEI 61131-3, c'est un programme qui peut être choisi pour être utilisé dans de nombreuses applications.

3.2.89
risque tolérable
risque accepté dans un certain contexte et fondé sur les valeurs actuelles de la société

NOTE Voir la CEI 61511-3.

[Guide ISO/CEI 51]

3.2.90
non détecté
non révélé
non déclaré
se rapporte aux anomalies de matériel et de logiciel, non détectées par les tests de diagnostic, ou lors de l'exploitation normale

NOTE Ce terme diffère de la définition donnée par la CEI 61508-4 pour refléter les différences dans la terminologie du domaine des processus.

3.2.91
validation
activité qui consiste à démontrer que la (les) fonction(s) instrumentée(s) de sécurité et le (les) système(s) instrumenté(s) de sécurité en question, après installation, satisfont en tous points à la spécification des exigences concernant la sécurité

3.2.92
vérification
activité qui consiste, pour chaque phase du cycle de vie de sécurité correspondant, à démontrer par analyse et/ou par essais, que, pour les entrées spécifiques, les sorties satisfont en tous points aux objectifs et aux exigences fixés pour la phase spécifique

NOTE Citons comme exemples d'activités de vérification:

– les revues relatives aux sorties d'une phase (documents concernant toutes les phases du cycle de vie de sécurité) destinées à assurer la conformité avec les objectifs et exigences de la phase, et prenant en compte les entrées spécifiques à cette phase;

– les revues de conception;

– les tests réalisés sur les produits mis au point, afin d'assurer que leur fonctionnement est conforme à leur spécification;

– les tests d'intégration réalisés lors de l'assemblage de différentes parties d'un système, élément par élément, et par la réalisation d'essais d'environnement, afin d'assurer que toutes les parties fonctionnent les unes avec les autres, conformément à ce qui est spécifié.

3.2.93
chien de garde
combinaison de diagnostics et d'un dispositif de sortie (typiquement un commutateur) pour effectuer la surveillance du bon fonctionnement du dispositif électronique programmable (PE) et entreprendre une action lors de la détection d'un fonctionnement incorrect

NOTE 1 Le chien de garde confirme que le système logiciel fonctionne correctement en réinitialisant régulièrement un dispositif externe (par exemple, temporisateur électronique de chien de garde matériel), par un dispositif de sortie commandé par le logiciel.

3.2.88
template
software template
structured non-specific piece of application software that can be easily altered to support specific functions while retaining the original structure; for example, an interactive screen template controls the process flow of the application screens, but is not specific to the data being presented; a programmer may take the generic template and make function-specific revisions to produce a new screen for the users

NOTE The related term "software template" is sometimes used. Typically, it refers to an algorithm or collection of algorithms that have been programmed to perform a desired function or set of functions and is constructed so it can be used in many different instances. In the context of IEC 61131-3, it is a program that can be selected for use in many applications.

3.2.89
tolerable risk
risk which is accepted in a given context based on the current values of society

NOTE See IEC 61511-3.

[ISO/IEC Guide 51]

3.2.90
undetected
unrevealed
covert
in relation to hardware and software faults not found by the diagnostic tests or during normal operation

NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.

3.2.91
validation
activity of demonstrating that the safety instrumented function(s) and safety instrumented system(s) under consideration after installation meets in all respects the safety requirements specification

3.2.92
verification
activity of demonstrating for each phase of the relevant safety life cycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase

NOTE Example verification activities include

– reviews on outputs (documents from all phases of the safety life cycle) to ensure compliance with the objectives and requirements of the phase taking into account the specific inputs to that phase;

– design reviews;

– tests performed on the designed products to ensure that they perform according to their specification;

– integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

3.2.93
watchdog
combination of diagnostics and an output device (typically a switch) for monitoring the correct operation of the programmable electronic (PE) device and taking action upon detection of an incorrect operation

NOTE 1 The watchdog confirms that the software system is operating correctly by the regular resetting of an external device (for example, hardware electronic watchdog timer) by an output device controlled by the software.

NOTE 2 Le chien de garde peut être utilisé pour désactiver un groupe de sorties de sécurité, lorsque des défaillances dangereuses sont détectées, afin de mettre le processus dans un état de sécurité. Le chien de garde est utilisé pour augmenter la couverture du diagnostic en ligne de l'unité logique de l'électronique programmable (PE) (voir 3.2.15 et 3.2.40).

4 Conformité à cette Norme internationale

Afin de se conformer à cette Norme internationale, il doit être montré que chacune des exigences décrites aux Articles 5 à 19 a été satisfaite par rapport aux critères définis, et que par conséquent, l'objectif ou les objectifs de l'Article a ou ont été atteint(s).

5 Gestion de la sécurité fonctionnelle

5.1 Objectif

L'objectif des exigences de cet article est d'identifier les activités de gestion qui sont nécessaires pour assurer que les objectifs de la sécurité fonctionnelle sont bien atteints.

NOTE Cet article a seulement pour but la réalisation et la maintenance de la sécurité fonctionnelle des systèmes instrumentés de sécurité; il est dissocié et distinct des mesures générales concernant la santé et la sécurité nécessaires pour l'obtention de la sécurité sur le lieu de travail.

5.2 Exigences

5.2.1 Généralités

5.2.1.1 La politique et la stratégie pour atteindre la sécurité doivent être identifiées, ainsi que les moyens pour évaluer sa réalisation, et doivent être communiquées au sein de l'organisation.

5.2.1.2 Un système de gestion de la sécurité doit être établi afin d'assurer que là où des systèmes instrumentés de sécurité sont utilisés, ils sont capables de mettre en place et/ou de maintenir le processus dans un état de sécurité.

5.2.2 Organisation et ressources

5.2.2.1 Les personnes, services, organisations et autres unités qui sont responsables de l'exécution et de la revue de chacune des phases du cycle de vie de sécurité doivent être identifiés et être informés des responsabilités qui leur sont affectées (y compris, lorsque cela est utile, les administrations d'autorisation ou les organismes de réglementation de la sécurité).

5.2.2.2 Les personnes, les services ou les organisations impliqués dans les activités du cycle de vie de sécurité doivent être compétents pour conduire les activités dont ils sont responsables.

NOTE Au minimum, il convient que les points suivants soient traités, en considérant la compétence des personnes, des services, des organisations ou des autres unités impliquées dans les activités du cycle de vie de sécurité:

a) connaissances d'ingénierie, formation et expérience appropriée concernant l'application de processus;

b) connaissances d'ingénierie, formation et expérience appropriée concernant la technologie applicable utilisée (par exemple, électrique, électronique, ou électronique programmable);

c) connaissances d'ingénierie, formation et expérience appropriée concernant les capteurs et les éléments terminaux;

d) connaissances d'ingénierie de la sécurité (par exemple, analyse de processus de sécurité);

e) connaissances des exigences légales et de celles régissant la sécurité;

f) gestion ad hoc et qualités de commandement appropriées à leur rôle dans les activités du cycle de vie de sécurité;

g) compréhension de la conséquence potentielle d'un événement;

h) niveau d'intégrité de sécurité des fonctions instrumentées de sécurité;

i) nouveauté et complexité de l'application et de la technologie.

NOTE 2 The watchdog can be used to de-energize a group of safety outputs when dangerous failures are detected in order to put the process into a safe state. The watchdog is used to increase the on-line diagnostic coverage of the PE logic solver (see 3.2.15 and 3.2.40).

4 Conformance to this International Standard

To conform to this International Standard , it shall be shown that each of the requirements outlined in Clauses 5 through 19 has been satisfied to the defined criteria and therefore the clause objective(s) has(have) been met.

5 Management of functional safety

5.1 Objective

The objective of the requirements of this clause is to identify the management activities that are necessary to ensure the functional safety objectives are met.

NOTE This clause is solely aimed at the achievement and maintenance of the functional safety of safety instrumented systems and is separate and distinct from general health and safety measures necessary for the achievement of safety in the workplace.

5.2 Requirements

5.2.1 General

5.2.1.1 The policy and strategy for achieving safety shall be identified together with the means for evaluating its achievement and shall be communicated within the organization.

5.2.1.2 A safety management system shall be in place so as to ensure that where safety instrumented systems are used, they have the ability to place and/or maintain the process in a safe state.

5.2.2 Organization and resources

5.2.2.1 Persons, departments, organizations or other units which are responsible for carrying out and reviewing each of the safety life-cycle phases shall be identified and be informed of the responsibilities assigned to them (including where relevant, licensing authorities or safety regulatory bodies).

5.2.2.2 Persons, departments or organizations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable.

NOTE As a minimum, the following items should be addressed when considering the competence of persons, departments, organizations or other units involved in safety life-cycle activities:

a) engineering knowledge, training and experience appropriate to the process application;

b) engineering knowledge, training and experience appropriate to the applicable technology used (for example, electrical, electronic or programmable electronic);

c) engineering knowledge, training and experience appropriate to the sensors and final elements;

d) safety engineering knowledge (for example, process safety analysis);

e) knowledge of the legal and safety regulatory requirements;

f) adequate management and leadership skills appropriate to their role in safety life-cycle activities;

g) understanding of the potential consequence of an event;

h) the safety integrity level of the safety instrumented functions;

i) the novelty and complexity of the application and the technology.

5.2.3 Évaluation et gestion des risques

5.2.3.1 Les dangers doivent être identifiés, les risques évalués et la réduction de risque nécessaire déterminée, comme cela est défini à l'Article 8.

NOTE Pour des raisons économiques, il peut être salutaire de considérer également les pertes potentielles en capital.

5.2.4 Planification

La planification de la sécurité doit être mise en place pour définir les activités qu'il est nécessaire d'effectuer avec les personnes, le service, l'organisation ou d'autres unités responsables, pour mener à bien ces activités. Cette planification doit être mise à jour dans son intégralité, selon les besoins, tout au long du cycle de vie de sécurité (voir l'Article 6).

NOTE La planification de la sécurité peut être incorporée dans:

– une section du plan qualité, intitulée «plan de sécurité» ou;

– un document séparé, intitulé «plan de sécurité» ou;

– plusieurs documents qui peuvent comprendre des procédures ou des méthodes de travail propres à la société.

5.2.5 Mise en oeuvre et surveillance

5.2.5.1 Des procédures doivent être mises en application pour assurer le suivi rapide et une prise en compte satisfaisante des recommandations ayant trait au système instrumenté de sécurité, et provenant:

a) De l'analyse de danger et l'évaluation des risques;

b) Des activités d'évaluation et d'audit;

c) Des activités de vérification;

d) Des activités de validation;

e) Des activités post-incident et post-accident.

5.2.5.2 Tous les fournisseurs, offrant des produits ou services à une organisation ayant une responsabilité globale pour l'une ou plusieurs des phases du cycle de vie de sécurité, doivent délivrer leurs produits ou services comme cela est spécifié par cette organisation et doivent posséder un système de gestion de la qualité. Les procédures doivent être en place pour établir l'adéquation du système de gestion de la qualité.

5.2.5.3 Les procédures doivent être mises en oeuvre pour évaluer les performances du système instrumenté de sécurité vis-à-vis de ses exigences de sécurité, y compris les procédures pour:

- l'identification et la prévention des défaillances systématiques qui pourraient compromettre la sécurité;
- évaluer si les taux des défaillances dangereuses du système instrumenté de sécurité sont conformes à ceux estimés lors de la conception;

  NOTE 1 Les défaillances dangereuses sont révélées au moyen de tests périodiques, de diagnostics ou de l'impossibilité de fonctionner sur une sollicitation.

  NOTE 2 Il convient de considérer que les procédures définissent l'action corrective nécessaire à entreprendre, si les taux des défaillances sont supérieurs à ceux qui ont été estimés lors de la conception.

- évaluer le taux de demande relatif aux fonctions instrumentées de sécurité, pendant le fonctionnement réel, pour vérifier les hypothèses faites lors de l'évaluation des risques, lorsque les exigences concernant le niveau d'intégrité ont été déterminées.

5.2.3 Risk evaluation and risk management

Hazards shall be identified, risks evaluated and the necessary risk reduction determined as defined in Clause 8.

NOTE It may be beneficial to consider also potential capital losses, for economical reasons.

5.2.4 Planning

Safety planning shall take place to define the activities that are required to be carried out along with the persons, department, organization or other units responsible to carry out these activities. This planning shall be updated as necessary throughout the entire safety life cycle (see Clause 6).

NOTE The safety planning may be incorporated in

– a section in the quality plan entitled “safety plan”; or

– a separate document entitled “safety plan”; or

– several documents which may include company procedures or working practices.

5.2.5 Implementing and monitoring

5.2.5.1 Procedures shall be implemented to ensure prompt follow-up and satisfactory resolution of recommendations pertaining to the safety instrumented system arising from

a) hazard analysis and risk assessment;

b) assessment and auditing activities;

c) verification activities;

d) validation activities;

e) post-incident and post-accident activities.

5.2.5.2 Any supplier, providing products or services to an organization, having overall responsibility for one or more phases of the safety life cycle, shall deliver products or services as specified by that organization and shall have a quality management system. Procedures shall be in place to establish the adequacy of the quality management system.

5.2.5.3 Procedures shall be implemented to evaluate the performance of the safety instrumented system against its safety requirements including procedures for

- identification and prevention of systematic failures which could jeopardize safety;
- assessing whether dangerous failure rates of the safety instrumented system are in accordance with those assumed during the design;

  NOTE 1 Dangerous failures are revealed by means of proof testing, diagnostics or failure to operate on demand.

  NOTE 2 Procedures should be considered that define the necessary corrective action to be taken if the failure rates are greater than what was assumed during design.
- assessing the demand rate on the safety instrumented functions during actual operation to verify the assumptions made during risk assessment when the integrity level requirements were determined.

5.2.6 Évaluation, audits et révisions

5.2.6.1 Evaluation de la sécurité fonctionnelle

5.2.6.1.1 Une procédure doit être définie et exécutée pour réaliser une évaluation de la sécurité fonctionnelle, de telle sorte qu'un jugement puisse être porté quant à la sécurité fonctionnelle et à l'intégrité de sécurité atteintes par le système instrumenté de sécurité. La procédure doit exiger qu'une équipe d'évaluation soit nommée; cette équipe doit avoir l'expertise technique, l'expertise de l'application et de l'exploitation, en adéquation avec l'installation en question.

5.2.6.1.2 L'équipe d'évaluation doit comprendre au moins une personne compétente de haut niveau, non impliquée dans l'équipe de conception de projet.

NOTE 1 Lorsque l'équipe d'évaluation est importante, il convient de porter attention au fait d'avoir plusieurs personnes de haut niveau et compétentes, dans l'équipe, indépendantes de l'équipe de projet.

NOTE 2 Il convient de considérer ce qui suit en planifiant une évaluation de la sécurité fonctionnelle:

– le domaine d'application de l'évaluation de la sécurité fonctionnelle;
– qui doit participer à l'évaluation de la sécurité fonctionnelle;
– les compétences, les responsabilités et les pouvoirs de l'équipe d'évaluation de la sécurité fonctionnelle;
– les informations devant être générées en tant que résultat de l'activité d'évaluation de la sécurité fonctionnelle;
– l'identité de tous les autres organismes de sécurité impliqués dans l'évaluation;
– les ressources requises pour conduire à son terme l'activité d'évaluation de la sécurité fonctionnelle;
– le niveau d'indépendance de l'équipe d'évaluation;
– les moyens par lesquels l'évaluation de la sécurité fonctionnelle doit être revalidée après des modifications.

5.2.6.1.3 Les étapes dans le cycle de vie de sécurité, auxquelles les activités d'évaluation de la sécurité fonctionnelles sont à effectuer, doivent être identifiées lors de la planification de la sécurité.

NOTE 1 Des activités additionnelles d'évaluation de la sécurité fonctionnelle peuvent devoir être introduites, en tant que nouveaux dangers identifiés après modification et à intervalles périodiques lors de l'exploitation.

NOTE 2 Il convient de porter une attention particulière à la mise en oeuvre des activités d'évaluation de la sécurité fonctionnelle aux étapes suivantes (voir la Figure 8):

– Étape 1 – Après avoir effectué l'évaluation des dangers et des risques, après avoir identifié les couches de protection requises et après avoir développé la spécification des exigences concernant la sécurité;
– Étape 2 – Après avoir conçu le système instrumenté de sécurité;
– Étape 3 – Après avoir terminé l'installation, la pré-mise en service et la validation finale du système instrumenté de sécurité et après avoir développé les procédures d'exploitation et de maintenance;
– Étape 4 – Après avoir acquis de l'expérience en exploitation et en maintenance;
– Étape 5 – Après des modifications et avant le déclassement du système instrumenté de sécurité.

NOTE 3 Le nombre, l'ampleur et le domaine d'application des activités d'évaluation de la sécurité fonctionnelle dépendent de circonstances particulières. Les facteurs intervenant dans cette décision sont susceptibles d'inclure:

– la taille du projet;
– le degré de complexité;
– le niveau d'intégrité de sécurité;
– la durée du projet;
– les conséquences en cas de défaillance;
– le degré de normalisation des particularités de conception;
– les exigences de réglementation de sécurité;
- l'expérience antérieure d'une conception de système similaire.

5.2.6 Assessment, auditing and revisions

5.2.6.1 Functional safety assessment

5.2.6.1.1 A procedure shall be defined and executed for a functional safety assessment in such a way that a judgement can be made as to the functional safety and safety integrity achieved by the safety instrumented system. The procedure shall require that an assessment team is appointed which includes the technical, application and operations expertise needed for the particular installation.

5.2.6.1.2 The membership of the assessment team shall include at least one senior competent person not involved in the project design team.

NOTE 1 When the assessment team is large, consideration should be given to having more than one senior competent individual on the team who is independent from the project team.

NOTE 2 The following should be considered when planning a functional safety assessment:

– the scope of the functional safety assessment;

– who is to participate in the functional safety assessment;

– the skills, responsibilities and authorities of the functional safety assessment team;

– the information that will be generated as a result of the functional safety assessment activity;

– the identity of any other safety bodies involved in the assessment;

– the resources required to complete the functional safety assessment activity;

– the level of independence of the assessment team;

– the means by which the functional safety assessment will be revalidated after modifications.

5.2.6.1.3 The stages in the safety life cycle at which the functional safety assessment activities are to be carried out shall be identified during safety planning.

NOTE 1 Additional functional safety assessment activities may need to be introduced as new hazards are identified, after modification and at periodic intervals during operation.

NOTE 2 Consideration should be given to carrying out functional safety assessment activities at the following stages (see Figure 8).

– Stage 1 - After the hazard and risk assessment has been carried out, the required protection layers have been identified and the safety requirement specification has been developed.

– Stage 2 - After the safety instrumented system has been designed.

– Stage 3 - After the installation, pre-commissioning and final validation of the safety instrumented system has been completed and operation and maintenance procedures have been developed.

– Stage 4 - After gaining experience in operating and maintenance.

– Stage 5 - After modification and prior to decommissioning of a safety instrumented system.

NOTE 3 The number, size and scope of functional safety assessment activities should depend upon the specific circumstances. The factors in this decision are likely to include

– size of project;

– degree of complexity;

– safety integrity level;

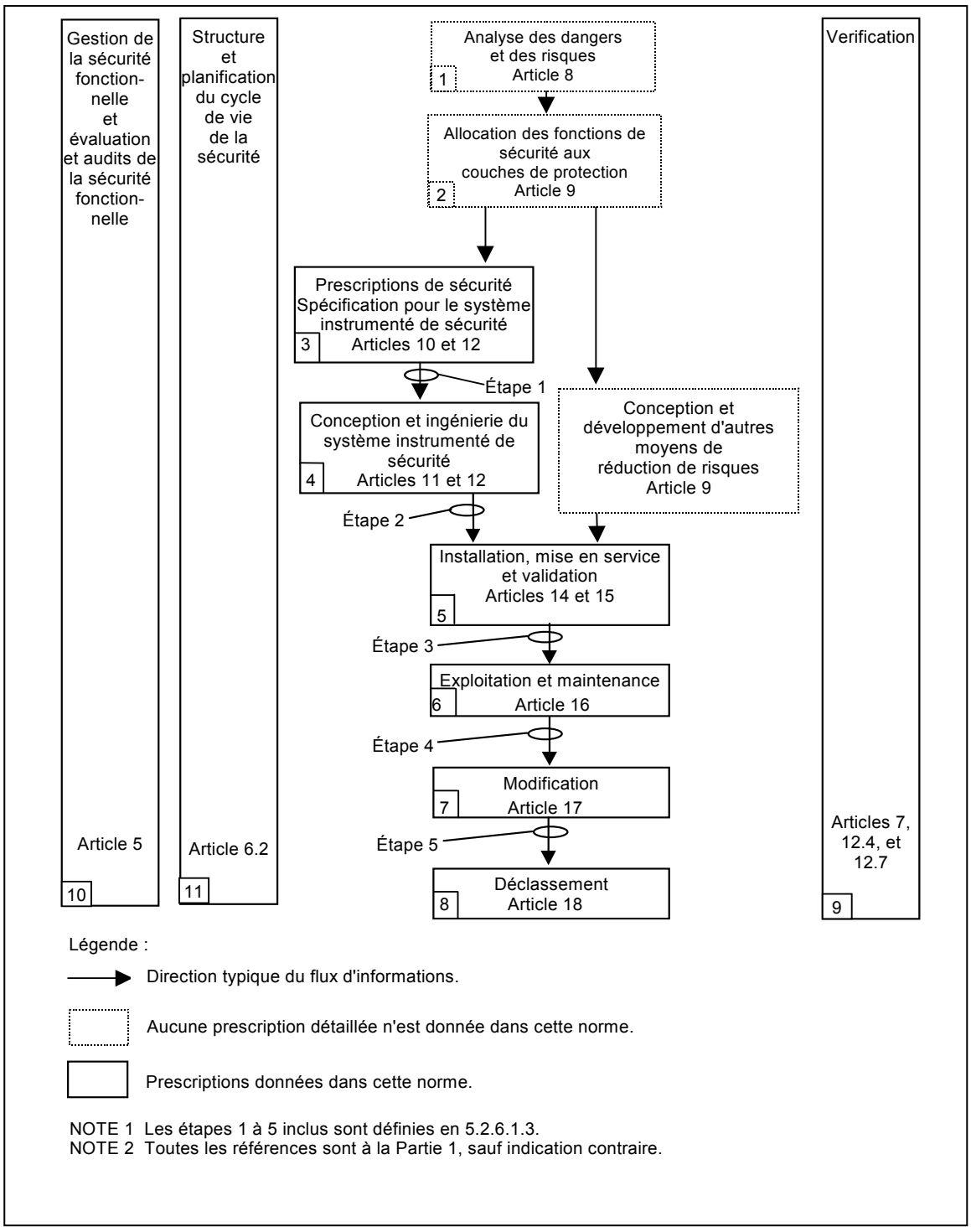
– duration of project;

– consequence in the event of failure;

– degree of standardization of design features;

– safety regulatory requirements;

– previous experience with a similar design.



IEC 3247/02

Figure 8 – Phases de cycle de vie de sécurité d'un SIS et étapes d'évaluation de la sécurité fonctionnelle

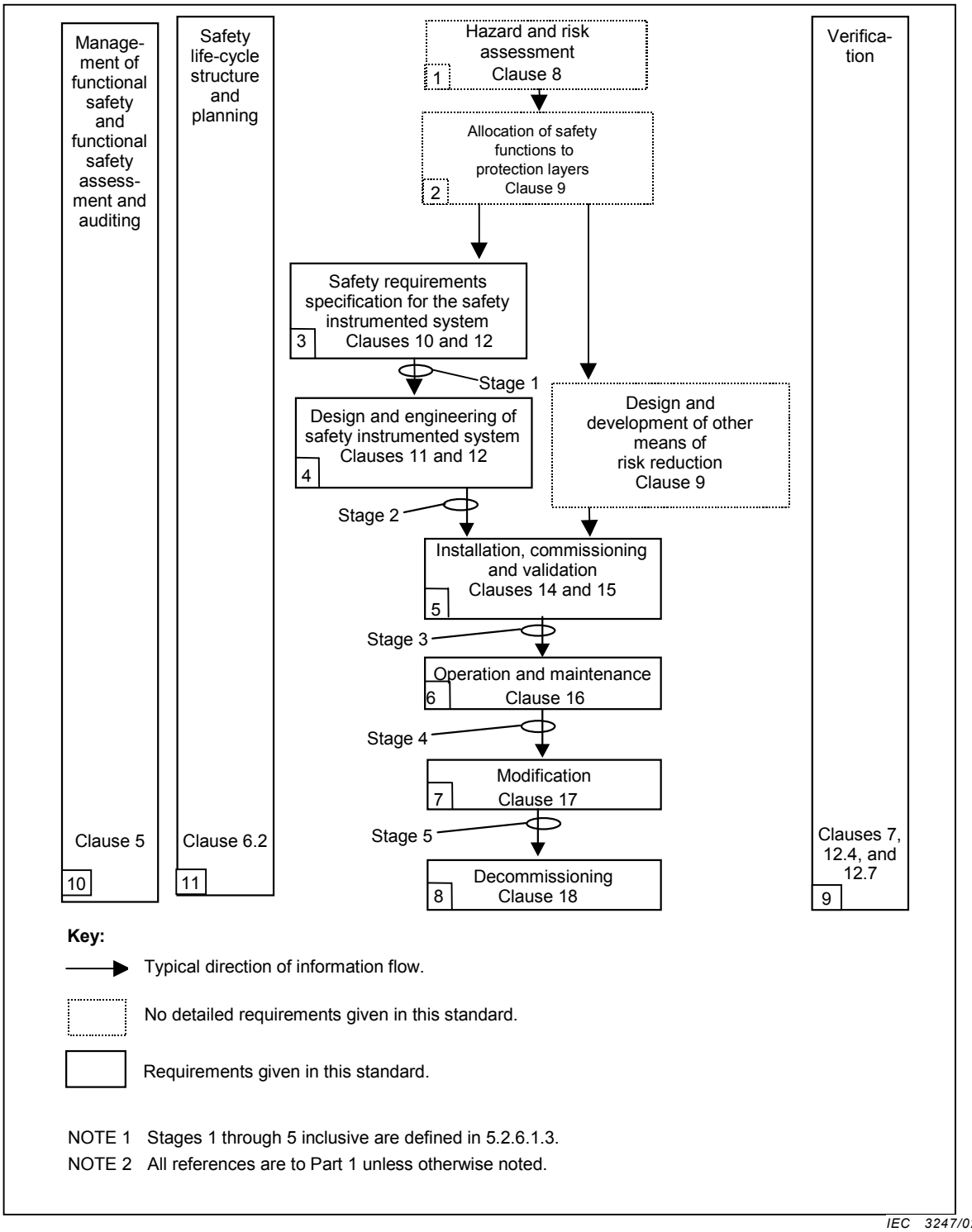


Figure 8 – SIS safety life-cycle phases and functional safety assessment stages

5.2.6.1.4 Au minimum une évaluation de la sécurité fonctionnelle doit être entreprise. Cette évaluation de la sécurité fonctionnelle doit être effectuée pour assurer que les dangers résultant d'un processus et de ses équipements associés sont correctement maîtrisés. Une évaluation doit être effectuée avant que les dangers identifiés ne soient présents (c'est-à-dire, à l'étape 3). L'équipe d'évaluation doit confirmer, avant que les dangers identifiés ne soient présents, que:

- l'évaluation des dangers et des risques a été effectuée (voir 8.1);
- les recommandations résultant de l'évaluation des dangers et des risques, qui s'appliquent au système instrumenté de sécurité, ont été mises en oeuvre ou prises en compte;
- les procédures de modification de conception du projet sont en place et ont été correctement mises en œuvre;
- les recommandations résultant de l'évaluation de la sécurité fonctionnelle précédente ont été prises en compte;
- le système instrumenté de sécurité est conçu, construit et installé selon la spécification des exigences concernant la sécurité, toutes les différences ayant été identifiées et prises en compte;
- les procédures de sécurité, d'exploitation, de maintenance et d'urgence, propres au système instrumenté de sécurité, sont en place;
- la planification de la validation du système instrumenté de sécurité est appropriée et que les activités de validation ont été conduites;
- la formation du personnel a été achevée et que les informations appropriées sur le système instrumenté de sécurité ont été fournies aux personnels de maintenance et exploitants;
- les stratégies ou les plans, pour mettre en oeuvre d'autres évaluations de la sécurité fonctionnelle, sont en place.

5.2.6.1.5 Dans le cas où des outils de développement et de production sont utilisés pour des activités du cycle de vie de sécurité, ils doivent eux-mêmes être soumis à une évaluation de la sécurité fonctionnelle.

NOTE 1 L'ampleur de l'utilisation qu'il convient de faire de ces outils dépendra de leur impact sur la sécurité à obtenir.

NOTE 2 Des exemples d'outils de développement et de production sont: les outils de simulation et de modélisation, les équipements d'essais, les équipements utilisés pendant les activités de maintenance et les outils de gestion de configuration.

NOTE 3 L'évaluation de la sécurité fonctionnelle des outils inclut, mais n'est pas limitée à, la traçabilité vis-à-vis des normes d'étalonnage, l'historique du fonctionnement et la liste des défauts.

5.2.6.1.6 Les résultats de l'évaluation de la sécurité fonctionnelle doivent être disponibles, ainsi que toutes les recommandations découlant de cette évaluation.

5.2.6.1.7 Toutes les informations pertinentes doivent être rendues disponibles, sur demande, pour l'équipe d'évaluation de la sécurité fonctionnelle.

5.2.6.2 Audits et révisions

5.2.6.2.1 Des procédures doivent être définies et exécutées pour auditer la conformité aux exigences, comprenant:

- la fréquence des activités d'audit;
- le degré de l'indépendance entre les personnes, les services, les organisations ou les autres unités effectuant le travail et ceux ou celles conduisant les activités d'audit;
- les activités d'enregistrement et de suivi.

5.2.6.1.4 At least one functional safety assessment shall be undertaken. This functional safety assessment shall be carried out to make sure the hazards arising from a process and its associated equipment are properly controlled. As a minimum, one assessment shall be carried out prior to the identified hazards being present (i.e., stage 3). The assessment team shall confirm, prior to the identified hazards being present, that

- the hazard and risk assessment has been carried out (see 8.1);
- the recommendations arising from the hazard and risk assessment that apply to the safety instrumented system have been implemented or resolved;
- project design change procedures are in place and have been properly implemented;
- the recommendations arising from the previous functional safety assessment have been resolved;
- the safety instrumented system is designed, constructed and installed in accordance with the safety requirement specification, any differences having been identified and resolved;
- the safety, operating, maintenance and emergency procedures pertaining to the safety instrumented system are in place;
- the safety instrumented system validation planning is appropriate and the validation activities have been completed;
- the employee training has been completed and appropriate information about the safety instrumented system has been provided to the maintenance and operating personnel;
- plans or strategies for implementing further functional safety assessments are in place.

5.2.6.1.5 Where development and production tools are used for any safety life-cycle activity, they shall themselves be subject to a functional safety assessment.

NOTE 1 The degree to which such tools should need to be addressed will depend upon their impact on the safety to be achieved.

NOTE 2 Examples of development and production tools include simulation and modelling tools, measuring equipment, test equipment, equipment used during maintenance activities and configuration management tools.

NOTE 3 Functional safety assessment of tools includes, but is not limited to, traceability to calibration standards, operating history and defect list.

5.2.6.1.6 The results of the functional safety assessment shall be available together with any recommendation coming from this assessment.

5.2.6.1.7 All relevant information shall be made available to the functional safety assessment team upon their request.

5.2.6.2 Auditing and revision

5.2.6.2.1 Procedures shall be defined and executed for auditing compliance with requirements including

- the frequency of the auditing activities;
- the degree of independence between the persons, departments, organizations or other units carrying out the work and those carrying out the auditing activities;
- the recording and follow-up activities.

5.2.6.2.2 La gestion des procédures de modification doit être en place pour initier, documenter, passer en revue, mettre en oeuvre et approuver les modifications au système instrumenté de sécurité, autres que le remplacement en nature (c'est-à-dire, à l'identique).

5.2.7 Gestion de configuration du SIS

5.2.7.1 Exigences

5.2.7.1.1 Les procédures de gestion de configuration du SIS pendant les phases du cycle de vie de sécurité du SIS et du logiciel doivent être disponibles; en particulier, il convient de spécifier les points suivants:

- l'étape à laquelle la maîtrise formelle de la configuration doit être mise en œuvre;
- les procédures à utiliser pour identifier de manière univoque toutes les parties constitutives d'une unité (matériel et logiciel);
- les procédures pour éviter que des éléments non autorisés n'entrent en service.

6 Exigences relatives au cycle de vie de sécurité

6.1 Objectifs

Les objectifs de cet article sont:

- définir les phases et établir les exigences relatives aux activités du cycle de vie de sécurité;
- organiser les activités techniques dans un cycle de vie de sécurité;
- assurer qu'une planification ad hoc existe ou est développée, ce qui permet d'être certain que le système instrumenté de sécurité satisfera aux exigences de sécurité.

NOTE L'approche globale de cette norme est illustrée par les Figures 8, 10 et 11. Il convient de souligner que cette approche est donnée à titre indicatif et n'est censée indiquer que les activités typiques du cycle de vie de sécurité, de la conception initiale, jusqu'au déclassement.

6.2 Exigences

6.2.1 Le cycle de vie de sécurité incorporant les exigences de cette norme doit être défini lors de la planification de la sécurité.

6.2.2 Chaque phase du cycle de vie de sécurité doit être définie en termes de ses entrées, de ses sorties et de ses activités de vérification (voir le Tableau 2).

5.2.6.2.2 Management of modification procedures shall be in place to initiate, document, review, implement and approve changes to the safety instrumented system other than replacement in kind (i.e. like for like).

5.2.7 SIS configuration management

5.2.7.1 Requirements

5.2.7.1.1 Procedures for configuration management of the SIS during the SIS and software safety life-cycle phases shall be available; in particular, the following should be specified:

- the stage at which formal configuration control is to be implemented;
- the procedures to be used for uniquely identifying all constituent parts of an item (hardware and software);
- the procedures for preventing unauthorized items from entering service.

6 Safety life-cycle requirements

6.1 Objectives

The objectives of this clause are:

- to define the phases and establish the requirements of the safety life-cycle activities;
- to organize the technical activities into a safety life cycle;
- to ensure that adequate planning exists (or is developed) that makes certain that the safety instrumented system shall meet the safety requirements.

NOTE The overall approach of this standard is shown in Figures 8, 10, and 11. It should be stressed that this approach is for illustration and is only meant to indicate the typical safety life-cycle activities from initial conception through decommissioning.

6.2 Requirements

6.2.1 A safety life-cycle incorporating the requirements of this standard shall be defined during safety planning.

6.2.2 Each phase of the safety life cycle shall be defined in terms of its inputs, outputs and verification activities (see Table 2).

Tableau 2 – Vue d'ensemble du cycle de vie de sécurité d'un SIS

Phase ou activité du cycle de vie de sécurité		Objectifs	Article des prescrip-tions	Entrées	Sorties
Numéro de case de la Figure 8	Titre				
1	Analyse de danger et de risque.	Déterminer les dangers et les événements dangereux du processus et des équipements associés, la séquence des événements conduisant à l'événement dangereux, les risques du processus associés à l'événement dangereux, les exigences concernant la réduction de risque et les fonctions de sécurité requises pour réaliser la réduction de risque nécessaire.	8	Conception du processus, agencement, équipes de personnel, cibles de sécurité.	Une description des dangers, de la (des) fonction(s) de sécurité requise(s) et de la réduction de risque associée.
2	Allocation des fonctions de sécurité aux couches de protection.	Allocation des fonctions de sécurité aux couches de protection et pour chaque fonction instrumentée de sécurité, le niveau d'intégrité de sécurité associé.	9	Description de la (des) fonction(s) de sécurité requise(s) et des exigences associées concernant l'intégrité de sécurité.	Description de l'allocation des exigences de sécurité (voir l'Article 9).
3	Spécification des exigences de sécurité du SIS.	Spécifier les exigences pour chaque SIS, en termes de fonctions instrumentées de sécurité requises et leur intégrité de sécurité associée, afin d'obtenir la sécurité fonctionnelle requise.	10	Description de l'allocation des exigences de sécurité (voir l'Article 9).	Exigences de sécurité du SIS; exigences de sécurité du logiciel.
4	Conception et ingénierie du SIS	Concevoir le SIS pour satisfaire aux exigences des fonctions instrumentées de sécurité et d'intégrité de sécurité.	11 et 12.4	Exigences de sécurité du SIS. Exigences de sécurité du logiciel.	Conception du SIS en conformité avec les exigences de sécurité du SIS; planification de l'essai d'intégration du SIS.
5	Installation, mise en service et validation du SIS	Intégrer et essayer le SIS. Valider que le SIS satisfait, en tous points, aux exigences de sécurité, en termes de fonctions instrumentées de sécurité et d'intégrité de sécurité requises.	12.3, 14, 15	Conception du SIS; Plan d'essai d'intégration du SIS. Exigences de sécurité du SIS. Plan de validation de sécurité du SIS	SIS fonctionnant entièrement en conformité avec les résultats des essais d'intégration du SIS, prévus à la conception du SIS. Résultats des activités d'installation, de mise en service et de validation.
6	Exploitation et maintenance du SIS.	Assurer que la sécurité fonctionnelle du SIS est conservée pendant l'exploitation et la maintenance.	16	Exigences du SIS; Conception du SIS. Plan pour l'exploitation et la maintenance du SIS.	Résultats des activités d'exploitation et de maintenance.

Table 2 – SIS safety life-cycle overview

Safety life-cycle phase or activity		Objectives	Require-ments	Inputs	Outputs
Figure 8 box number	Title		Clause or subclause		
1	Hazard and risk assessment	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction	8	Process design, layout, manning arrangements, safety targets	A description of the hazards, of the required safety function(s) and of the associated risk reduction
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each safety instrumented function, the associated safety integrity level	9	A description of the required safety instrumented function(s) and associated safety integrity requirements	Description of allocation of safety requirements (see Clause 9)
3	SIS safety requirements specification	To specify the requirements for each SIS, in terms of the required safety instrumented functions and their associated safety integrity, in order to achieve the required functional safety	10	Description of allocation of safety requirements (see clause 9)	SIS safety requirements; software safety requirements
4	SIS design and engineering	To design the SIS to meet the requirements for safety instrumented functions and safety integrity	11 and 12.4	SIS safety requirements Software safety requirements	Design of the SIS in conformance with the SIS safety requirements; planning for the SIS integration test
5	SIS installation commissioning and validation	To integrate and test the SIS To validate that the SIS meets in all respects the requirements for safety in terms of the required safety instrumented functions and the required safety integrity	12.3, 14, 15	SIS design SIS integration test plan SIS safety requirements Plan for the safety validation of the SIS	Fully functioning SIS in conformance with the SIS design results of SIS integration tests Results of the installation, com-missioning and validation activities
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	16	SIS requirements SIS design Plan for SIS operation and maintenance	Results of the operation and maintenance activities

Phase ou activité du cycle de vie de sécurité		Objectifs	Article des prescrip-tions	Entrées	Sorties
Numéro de case de la Figure 8	Titre				
7	Modifications au SIS.	Faire des corrections, des améliorations ou des adaptations au SIS, en s'assurant que le niveau d'intégrité de sécurité requis est obtenu et maintenu.	17	Exigences de sécurité du SIS révisées.	Résultats des modifications au SIS.
8	Déclassement.	Assurer la revue, l'organisation sectorielle ad hoc, et assurer que la SIF reste appropriée.	18	Exigences de sécurité et informations de processus conformes à la construction.	SIF déclaré hors service.
9	Vérification du SIS.	Essayer et évaluer les sorties d'une phase donnée, pour assurer la véracité et la cohérence par rapport aux produits et aux normes donnés comme entrées à cette phase.	7, 12.7	Plan de vérification du SIS, pour chaque phase.	Résultats de la vérification du SIS, pour chaque phase.
10	Évaluation de la sécurité fonctionnelle du SIS.	Enquêter et arriver à un jugement sur la sécurité fonctionnelle obtenue par le SIS.	5	Planification de l'évaluation de la sécurité fonctionnelle du SIS. Prescription de sécurité du SIS.	Résultats de l'évaluation de la sécurité fonctionnelle du SIS.

6.2.3 Pour toutes les phases du cycle de vie de sécurité, la planification de la sécurité doit avoir lieu pour définir les critères, les techniques, les mesures et les procédures afin de:

- assurer que les exigences de sécurité du SIS sont tenues pour tous les modes concernés du processus; ceci inclut à la fois les exigences fonctionnelles de sécurité et les exigences concernant l'intégrité de la sécurité;
- assurer l'installation et la mise en service appropriées du système instrumenté de sécurité;
- assurer l'intégrité de la sécurité des fonctions instrumentées de sécurité après l'installation;
- maintenir l'intégrité de la sécurité lors de l'exploitation (par exemple, tests périodiques, analyse des défaillances);
- gérer les dangers du processus pendant les activités de maintenance sur le système instrumenté de sécurité.

Table 2 *(continued)*

Safety life-cycle phase or activity		Objectives	Require-ments Clause or subclause	Inputs	Outputs
Figure 8 box number	Title				
7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required safety integrity level is achieved and maintained	17	Revised SIS safety requirements	Results of SIS modification
8	Decommission-ing	To ensure proper review, sector organization, and ensure SIF remain appropriate	18	As built safety requirements and process information	SIF placed out of service
9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	7, 12.7	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase
10	SIS functional safety assessment	To investigate and arrive at a judgement on the functional safety achieved by the SIS	5	Planning for SIS functional safety assessment SIS safety requirement	Results of SIS functional safety assessment

6.2.3 For all safety life-cycle phases, safety planning shall take place to define the criteria, techniques, measures and procedures to

- ensure that the SIS safety requirements are achieved for all relevant modes of the process; this includes both function and safety integrity requirements;
- ensure proper installation and commissioning of the safety instrumented system;
- ensure the safety integrity of the safety instrumented functions after installation;
- maintain the safety integrity during operation (for example, proof testing, failure analysis);
- manage the process hazards during maintenance activities on the safety instrumented system.

7 Vérification

7.1 Objectifs

L'objectif de cet article est de démontrer par revue, analyse et/ou essais, que les sorties requises satisfont aux exigences définies pour les phases appropriées (Figure 8) du cycle de vie de sécurité, identifiées par la planification de la vérification.

7.1.1 Exigences

La planification de la vérification doit définir toutes les activités demandées pour la phase appropriée (Figure 8) du cycle de vie de sécurité. Elle doit être conforme à cette norme, en fournissant les informations suivantes:

- les activités de vérification;
- les procédures, les mesures et les techniques à utiliser pour la vérification, comprenant la mise en oeuvre et la prise en compte des recommandations résultantes;
- le moment où ces activités auront lieu dans le temps;
- les personnes, les services et les organisations responsables de ces activités, y compris les niveaux d'indépendance;
- l'identification des éléments à vérifier;
- l'identification des informations vis-à-vis desquelles la vérification est effectuée;
- comment appréhender les non-conformités;
- les outils et l'analyse justificative.

7.1.1.1 La vérification doit être effectuée en accord avec la planification de la vérification.

7.1.1.2 Les résultats de la procédure de vérification doivent être disponibles.

NOTE 1 Le choix des techniques et des mesures concernant la procédure de vérification et le degré d'indépendance dépend d'un certain nombre de facteurs, comprenant le degré de complexité, d'innovation de la conception, d'innovation de la technologie et du niveau d'intégrité de sécurité exigé.

NOTE 2 On peut citer des exemples de certaines activités de vérification telles que les revues de conception, l'utilisation d'outils et de techniques, comprenant des outils de vérification de logiciel et des outils de DAO.

8 Analyse de danger et de risque relatifs au processus

8.1 Objectifs

Les objectifs des exigences de cet article sont de déterminer:

- les dangers et les événements dangereux du processus et des équipements associés;
- l'enchaînement des événements conduisant à l'événement dangereux;
- les risques relatifs au processus, associés à l'événement dangereux;
- toutes les exigences concernant la réduction des risques;
- les fonctions de sécurité requises pour atteindre la réduction de risque nécessaire;
- si l'une des fonctions de sécurité est une fonction instrumentée de sécurité (voir l'Article 9).

NOTE 1 L'Article 8 de cette norme s'adresse aux ingénieurs de processus, aux spécialistes en danger et en risque, aux directeurs de la sécurité, ainsi qu'aux ingénieurs instrumentistes. Le but est de prendre en compte l'approche multidisciplinaire habituellement requise pour la détermination des fonctions instrumentées de sécurité.

NOTE 2 Lorsque cela est réalisable, il convient que les processus soient conçus pour présenter une sécurité intrinsèque. Lorsque cela n'est pas réalisable, des méthodes de réduction de risque, telles que des systèmes de protection mécaniques et des systèmes instrumentés de sécurité peuvent devoir être ajoutés à la conception. Ces systèmes peuvent agir seuls ou associés entre eux.

7 Verification

7.1 Objective

The objective of this clause is to demonstrate by review, analysis and/or testing that the required outputs satisfy the defined requirements for the appropriate phases (Figure 8) of the safety life cycle identified by the verification planning.

7.1.1 Requirements

Verification planning shall define all activities required for the appropriate phase (Figure 8) of the safety life cycle. It shall conform to this standard by providing the following:

- the verification activities;
- the procedures, measures and techniques to be used for verification including implementation and resolution of resulting recommendations;
- when these activities will take place;
- the persons, departments and organizations responsible for these activities, including levels of independence;
- identification of items to be verified;
- identification of the information against which the verification is carried out;
- how to handle non-conformances;
- tools and supporting analysis.

7.1.1.1 Verification shall be performed according to the verification planning.

7.1.1.2 The results of the verification process shall be available.

NOTE 1 Selection of techniques and measures for the verification process and the degree of independence depends upon a number of factors including degree of complexity, novelty of design, novelty of technology and safety integrity level required.

NOTE 2 Examples of some verification activities include design reviews, use of tools and techniques including software verification tools and CAD tools.

8 Process hazard and risk assessment

8.1 Objectives

The objectives of the requirements of this clause are:

- to determine the hazards and hazardous events of the process and associated equipment;
- to determine the sequence of events leading to the hazardous event;
- to determine the process risks associated with the hazardous event;
- to determine any requirements for risk reduction;
- to determine the safety functions required to achieve the necessary risk reduction;
- to determine if any of the safety functions are safety instrumented functions (see Clause 9).

NOTE 1 Clause 8 of this standard is addressed to process engineers, hazard and risk specialists, safety managers as well as instrument engineers. The purpose is to recognize the multi-disciplinary approach typically required for the determination of safety instrumented functions.

NOTE 2 Where reasonably practicable, processes should be designed to be inherently safe. When this is not practical, risk reduction methods such as mechanical protection systems and safety instrumented systems may need to be added to the design. These systems may act alone or in combination with each other.

NOTE 3 Les méthodes habituelles de réduction de risque rencontrées dans les industries de processus sont indiquées à la Figure 9 (sans aucune hiérarchie implicite).

8.2 Exigences

8.2.1 Une analyse de danger et de risque doit être effectuée sur le processus et ses équipements associés (par exemple, un BPCS). Elle aura comme résultat:

- une description de chaque événement dangereux identifié et des facteurs qui y contribuent (erreurs humaines y compris);
- une description des conséquences et de la probabilité de l'événement;
- la prise en compte des conditions, telles que l'exploitation normale, la mise en route, l'arrêt, la maintenance, la perte de contrôle du processus, l'arrêt d'urgence;
- la détermination des exigences relatives à la réduction de risque supplémentaire nécessaire pour atteindre la sécurité requise;
- une description, ou des références à des informations concernant les mesures prises pour réduire ou éliminer les dangers et le risque;
- une description détaillée des hypothèses faites pendant l'analyse des risques, comprenant les taux probables de sollicitation et les taux de défaillance des équipements, ainsi que toute prise en compte de contraintes opérationnelles ou d'intervention humaine;
- l'allocation des fonctions de sécurité aux couches de protection (voir l'Article 9), en tenant compte de la réduction potentielle de la protection effective due à une défaillance de cause commune, entre couches de sécurité et entre les couches de sécurité et le BPCS (voir la note 1);
- l'identification de la (des) fonction(s) de sécurité appliquée(s) en tant que fonction(s) instrumentée(s) de sécurité (voir l'Article 9).

NOTE 1 Lors de la détermination des exigences concernant l'intégrité de sécurité, il sera nécessaire de tenir compte des effets de la cause commune entre les systèmes qui créent les sollicitations et les systèmes de protection qui sont conçus pour répondre à ces sollicitations. Un exemple de ceci est illustré par le cas où les sollicitations peuvent survenir de par une défaillance du système de commande et les équipements utilisés dans les systèmes de protection sont semblables ou identiques aux équipements utilisés dans le système de commande. Dans de tels cas, il ne peut être répondu efficacement à une sollicitation provoquée par une défaillance d'équipement dans le système de commande, si une cause commune a rendu inefficace l'équipement similaire dans le système de protection. Il se peut que des problèmes de cause commune ne puissent pas être pris en compte pendant l'identification initiale des dangers et de l'analyse de risque, parce qu'à cette première étape, la conception du système de protection n'a pas été nécessairement terminée. Dans ce cas, il sera nécessaire de reconsidérer les exigences concernant l'intégrité de sécurité et la fonction instrumentée de sécurité, une fois que la conception du système instrumenté de sécurité et des autres couches de protection aura été achevée. En déterminant si la conception globale du processus et des couches de protection satisfait ou non aux exigences, il sera nécessaire de considérer les défaillances de cause commune.

NOTE 2 Les exemples de techniques qui peuvent être utilisées pour établir le SIL prescrit, relatif aux fonctions instrumentées de sécurité, sont présentés dans la CEI 61511-3.

8.2.2 Le taux des défaillances dangereuses d'un BPCS (qui n'est pas conforme à la CEI 61511), qui entraîne une sollicitation d'une couche de protection, ne doit pas être estimé à une valeur supérieure à 10^{-5} par heure.

8.2.3 L'évaluation de danger et de risque doit être consignée de telle manière que la relation entre les éléments ci-dessus soit claire et traçable.

NOTE 1 Les exigences ci-dessus n'exigent pas que les cibles de réduction de danger et de risque soient affectées en tant que valeur numérique. Des approches graphiques (voir la CEI 61511-3) peuvent également être utilisées.

NOTE 2 Il convient que l'ampleur de la réduction de risque nécessaire puisse varier selon l'application et les exigences nationales légales. Un principe admis dans de nombreux pays est qu'il convient que les mesures de réduction de risque supplémentaires soient appliquées jusqu'à ce que le coût engagé devienne disproportionné par rapport à la réduction de risque obtenue.

NOTE 3 Typical risk reduction methods found in process plants are indicated in Figure 9 (no hierarchy implied).

8.2 Requirements

8.2.1 A hazard and risk assessment shall be carried out on the process and its associated equipment (for example, BPCS). It shall result in

- a description of each identified hazardous event and the factors that contribute to it (including human errors);
- a description of the consequences and likelihood of the event;
- consideration of conditions such as normal operation, start-up, shutdown, maintenance, process upset, emergency shutdown;
- the determination of requirements for additional risk reduction necessary to achieve the required safety;
- a description of, or references to information on, the measures taken to reduce or remove hazards and risk;
- a detailed description of the assumptions made during the analysis of the risks including probable demand rates and equipment failure rates, and of any credit taken for operational constraints or human intervention;
- allocation of the safety functions to layers of protection (see Clause 9) taking account of potential reduction in effective protection due to common cause failure between the safety layers and between the safety layers and the BPCS (see note 1);
- identification of those safety function(s) applied as safety instrumented function(s) (see Clause 9).

NOTE 1 In determining the safety integrity requirements, account will need to be taken of the effects of common cause between systems that create demands and the protection systems that are designed to respond to those demands. An example of this would be where demands can arise through control system failure and the equipment used within the protection systems is similar or identical to the equipment used within the control system. In such cases, a demand caused by a failure of equipment in the control system may not be responded to effectively if a common cause has rendered similar equipment in the protection system to be ineffective. It may not be possible to recognize common cause problems during the initial hazard identification and risk analysis because at such an early stage the design of the protection system will not necessarily have been completed. In such cases, it will be necessary to reconsider the requirements for safety integrity and safety instrumented function once the design of the safety instrumented system and other layers of protection has been completed. In determining whether the overall design of process and protection layers meets requirements, common cause failures will need to be considered.

NOTE 2 Examples of techniques that can be used to establish the required SIL of safety instrumented functions are illustrated in IEC 61511-3.

8.2.2 The dangerous failure rate of a BPCS (which does not conform to IEC 61511) that places a demand on a protection layer shall not be assumed to be better than 10^{-5} per hour.

8.2.3 The hazard and risk assessment shall be recorded in such a way that the relationship between the above items is clear and traceable.

NOTE 1 The above requirements do not mandate that risk and risk reduction targets have to be assigned as numerical value. Graphical approaches (see IEC 61511-3) can also be used.

NOTE 2 The extent of risk reduction necessary should vary depending on the application and national legal requirements. An accepted principle in many countries is that additional risk reduction measures should be applied until the cost incurred becomes disproportionate to the risk reduction achieved.

9 Allocation des fonctions de sécurité aux couches de protection

9.1 Objectifs

Les objectifs des exigences de cet article sont:

- D'allouer les fonctions de sécurité aux couches de protection,
- De déterminer les fonctions instrumentées de sécurité requises,
- De déterminer, pour chaque fonction instrumentée de sécurité, le niveau d'intégrité de sécurité associé.

NOTE Il convient de prendre en compte, pendant le processus d'allocation, des autres standards ou pratiques de l'industrie.

9.2 Exigences relatives au processus d'allocation

9.2.1 Le processus d'allocation doit avoir comme résultat:

- l'allocation des fonctions de sécurité aux couches de protection spécifiques dans un but de prévention, de maîtrise ou d'atténuation des dangers provenant du processus et de ses équipements associés;
- l'allocation des cibles de réduction de risque aux fonctions instrumentées de sécurité.

NOTE Les exigences légales ou d'autres pratiques de l'industrie peuvent déterminer des priorités dans le processus d'allocation.

9.2.2 Le niveau d'intégrité de sécurité exigé d'une fonction instrumentée de sécurité doit être obtenu en tenant compte de la réduction de risque requise, à fournir par cette fonction.

NOTE Voir la CEI 61511-3 qui donne des lignes directrices.

9.2.3 Pour chaque fonction instrumentée de sécurité fonctionnant en mode de sollicitation, le SIL requis doit être spécifié en accord avec le Tableau 3 ou le Tableau 4. Si le Tableau 4 est utilisé, alors ni l'intervalle de test périodique, ni le taux de sollicitation ne doivent être utilisés dans la détermination du niveau d'intégrité de sécurité.

9.2.4 Pour chaque fonction instrumentée de sécurité fonctionnant en mode continu de fonctionnement, le SIL requis doit être spécifié en accord avec le Tableau 4.

Tableau 3 – Niveaux d'intégrité de sécurité: probabilité de défaillance lors d'une sollicitation

FONCTIONNEMENT EN MODE SOLLICITATION		
Niveau d'intégrité de sécurité (SIL)	**Probabilité de défaillance moyenne cible lors d'une sollicitation**	**Réduction de risque cible**
4	$\geq 10^{-5}$ à $<10^{-4}$	>10 000 à ≤ 100 000
3	$\geq 10^{-4}$ à $<10^{-3}$	>1 000 à ≤ 10 000
2	$\geq 10^{-3}$ à $<10^{-2}$	>100 à ≤ 1000
1	$\geq 10^{-2}$ à $<10^{-1}$	>10 à ≤ 100

9 Allocation of safety functions to protection layers

9.1 Objectives

The objectives of the requirements of this clause are to

- allocate safety functions to protection layers;
- determine the required safety instrumented functions;
- determine, for each safety instrumented function, the associated safety integrity level.

NOTE Account should be taken, during the process of allocation, of other industry standards or codes.

9.2 Requirements of the allocation process

9.2.1 The allocation process shall result in

- the allocation of safety functions to specific protection layers for the purpose of prevention, control or mitigation of hazards from the process and its associated equipment;
- the allocation of risk reduction targets to safety instrumented functions.

NOTE Legislative requirements or other industry codes may determine priorities in the allocation process.

9.2.2 The required safety integrity level of a safety instrumented function shall be derived by taking into account the required risk reduction that is to be provided by that function.

NOTE See IEC 61511-3 for guidance.

9.2.3 For each safety instrumented function operating in demand mode, the required SIL shall be specified in accordance with either Table 3 or Table 4. If Table 4 is used then neither the proof-test interval nor the demand rate shall be used in the determination of safety integrity level.

9.2.4 For each safety instrumented function operating in continuous mode of operation, the required SIL shall be specified in accordance with Table 4.

Table 3 – Safety integrity levels: probability of failure on demand

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	**Target average probability of failure on demand**	**Target risk reduction**
4	$\geq 10^{-5}$ to $< 10^{-4}$	>10 000 to ≤100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	>1 000 to ≤10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	>100 to ≤1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	>10 to ≤100

Tableau 4 – Niveaux d'intégrité de sécurité: probabilité des défaillances dangereuses de la SIF

FONCTIONNEMENT EN MODE CONTINU	
Niveau d'intégrité de sécurité (SIL)	**Probabilité cible des défaillances dangereuses pour exécuter la fonction instrumentée de sécurité (par heure)**
4	$\geq 10^{-9}$ à $<10^{-8}$
3	$\geq 10^{-8}$ à $<10^{-7}$
2	$\geq 10^{-7}$ à $<10^{-6}$
1	$\geq 10^{-6}$ à $<10^{-5}$

NOTE 1 Voir 3.2.43 pour d'autres d'explications.

NOTE 2 Le niveau d'intégrité de sécurité est défini numériquement afin de fournir une cible objective pour comparer des conceptions et des solutions alternatives. Cependant, il est reconnu qu'étant donné l'état actuel des connaissances, de nombreuses causes systématiques de défaillance ne peuvent être évaluées que qualitativement.

NOTE 3 La probabilité maximale des défaillances dangereuses par heure requise pour une fonction instrumentée de sécurité en mode continu est déterminée en considérant le risque (en termes de taux de danger) provoqué par une défaillance de la fonction instrumentée de sécurité agissant en mode continu, ainsi que le taux de défaillance d'autres équipements, ce qui conduit au même risque, en prenant en considération des contributions issues d'autres couches de protection.

NOTE 4 Il est possible d'utiliser plusieurs systèmes de niveau d'intégrité de sécurité inférieurs pour satisfaire au besoin d'une fonction de niveau plus élevée (par exemple, en utilisant un système à la fois de SIL 2 et de SIL 1 pour satisfaire au besoin d'une fonction de SIL 3).

9.3 Exigences supplémentaires pour le niveau 4 d'intégrité de sécurité

9.3.1 Aucune fonction instrumentée de sécurité, ayant un niveau d'intégrité de sécurité supérieur à celui associé au SIL 4, ne doit être allouée à un système instrumenté de sécurité. Les applications, qui nécessitent l'utilisation d'une fonction instrumentée de sécurité unique du niveau 4 d'intégrité de sécurité, sont rares dans l'industrie des processus. Ces applications doivent être évitées, lorsque cela est raisonnablement possible, en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie de sécurité. Dans les cas où de tels systèmes sont spécifiés, toutes les personnes qui sont impliquées dans le cycle de vie de sécurité devront avoir des niveaux de compétence élevés.

Si l'analyse détermine qu'un niveau d'intégrité de sécurité de 4 a été affecté à une fonction instrumentée de sécurité, la conception du processus doit être reconsidérée de manière à ce qu'il devienne en lui-même plus sûr ou que des couches supplémentaires de protection soient ajoutées. Ces améliorations peuvent peut-être réduire les exigences de niveau d'intégrité de sécurité pour la fonction instrumentée de sécurité.

9.3.2 Une fonction instrumentée de sécurité de niveau 4 d'intégrité de sécurité ne doit être permise que si les critères du point a) ou des points b) et c) (considérés ensemble) ci-dessous sont remplis:

a) il existe une démonstration explicite, par combinaison de méthodes analytiques et d'essais appropriés, de l'atteinte de l'objectif du niveau de défaillance d'intégrité de sécurité;

b) on possède une expérience significative en exploitation, des composants utilisés au sein de la fonction instrumentée de sécurité;

NOTE Il convient que cette expérience ait été acquise dans un environnement similaire et, au minimum, il convient que les composants aient été utilisés dans un système de niveau de complexité comparable.

c) on possède suffisamment de données de défaillance matérielle, obtenues à partir des composants utilisés au sein de la fonction instrumentée de sécurité, pour accorder une confiance satisfaisante dans l'objectif du niveau de défaillance d'intégrité de sécurité du matériel, qui est à tenir.

NOTE Il convient d'utiliser des données appropriées à l'environnement proposé, à l'application et au niveau de complexité.

Table 4 – Safety integrity levels: frequency of dangerous failures of the SIF

CONTINUOUS MODE OF OPERATION	
Safety integrity level (SIL)	**Target frequency of dangerous failures to perform the safety instrumented function (per hour)**
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

NOTE 1 See 3.2.43 for further explanation.

NOTE 2 The safety integrity level is defined numerically so as to provide an objective target to compare alternative designs and solutions. However, it is recognized that, given the current state of knowledge, many systematic causes of failure can only be assessed qualitatively.

NOTE 3 The required frequency of dangerous failures per hour for a continuous mode safety instrumented function is determined by considering the risk (in terms of hazard rate) caused by failure of the safety instrumented function acting in continuous mode together with the failure rate of other equipment that leads to the same risk, taking into consideration contributions from other protection layers.

NOTE 4 It is possible to use several lower safety integrity level systems to satisfy the need for a higher level function (for example, using a SIL 2 and a SIL 1 system together to satisfy the need for a SIL 3 function).

9.3 Additional requirements for safety integrity level 4

9.3.1 No safety instrumented function with a safety integrity level higher than that associated with SIL 4 shall be allocated to a safety instrumented system. Applications which require the use of a single safety instrumented function of safety integrity level 4 are rare in the process industry. Such applications shall be avoided where reasonably practicable because of the difficulty of achieving and maintaining such high levels of performance throughout the safety life cycle. Where such systems are specified they will require high levels of competence from all those involved throughout the safety life cycle.

If the analysis results in a safety integrity level of 4 being assigned to a safety instrumented function, consideration shall be given to changing the process design in such a way that it becomes more inherently safe or adding additional layers of protection. These enhancements could perhaps then reduce safety integrity level requirements for the safety instrumented function.

9.3.2 A safety instrumented function of safety integrity level 4 shall be permitted only if the criteria in either a), or both b) and c) below are met.

a) There has been an explicit demonstration, by a combination of appropriate analytical methods and testing, of the target safety integrity failure measure having been met.

b) There has been extensive operating experience of the components used as part of the safety instrumented function.

   NOTE Such experience should have been gained in a similar environment and, as a minimum, components should have been used in a system of comparable complexity level.

c) There is sufficient hardware failure data, obtained from components used as part of the safety instrumented function, to allow sufficient confidence in the hardware safety integrity target failure measure that is to be claimed.

   NOTE The data should be relevant to the proposed environment, application and complexity level.

9.4 Exigences relatives au système de commande de processus de base en tant que couche de protection

9.4.1 Le système de commande processus de base peut être identifié en tant que couche de protection, comme cela est représenté à la Figure 9.

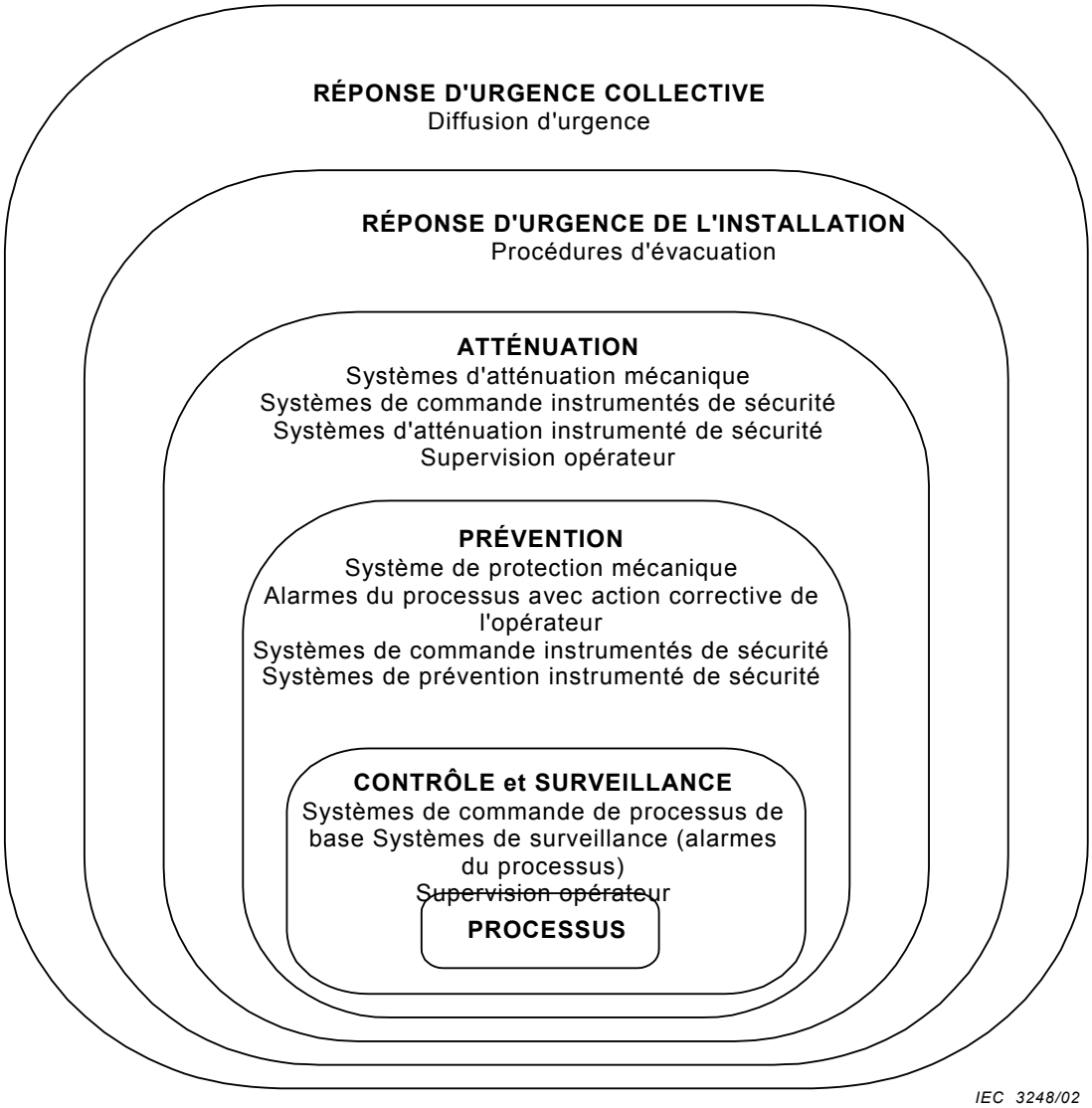


Figure 9 – Méthodes habituelles de réduction de risque rencontrées dans les industries de processus

9.4.2 Le facteur de réduction de risque pour un BPCS (qui n'est pas conforme à la CEI 61511 ou à la CEI 61508) utilisé comme couche de protection, doit être inférieur à 10.

NOTE En considérant le crédit de réduction de risque que l'on peut accorder à un BPCS, il convient de prendre en compte le fait qu'une partie du BPCS peut également être une source de déclenchement d'un événement.

9.4.3 Si un facteur de réduction de risque supérieur à 10 est annoncé pour le BPCS, ce dernier doit alors être conçu pour satisfaire aux exigences de cette norme.

9.4 Requirements on the basic process control system as a protection layer

9.4.1 The basic process control system may be identified as a protection layer as shown in Figure 9.

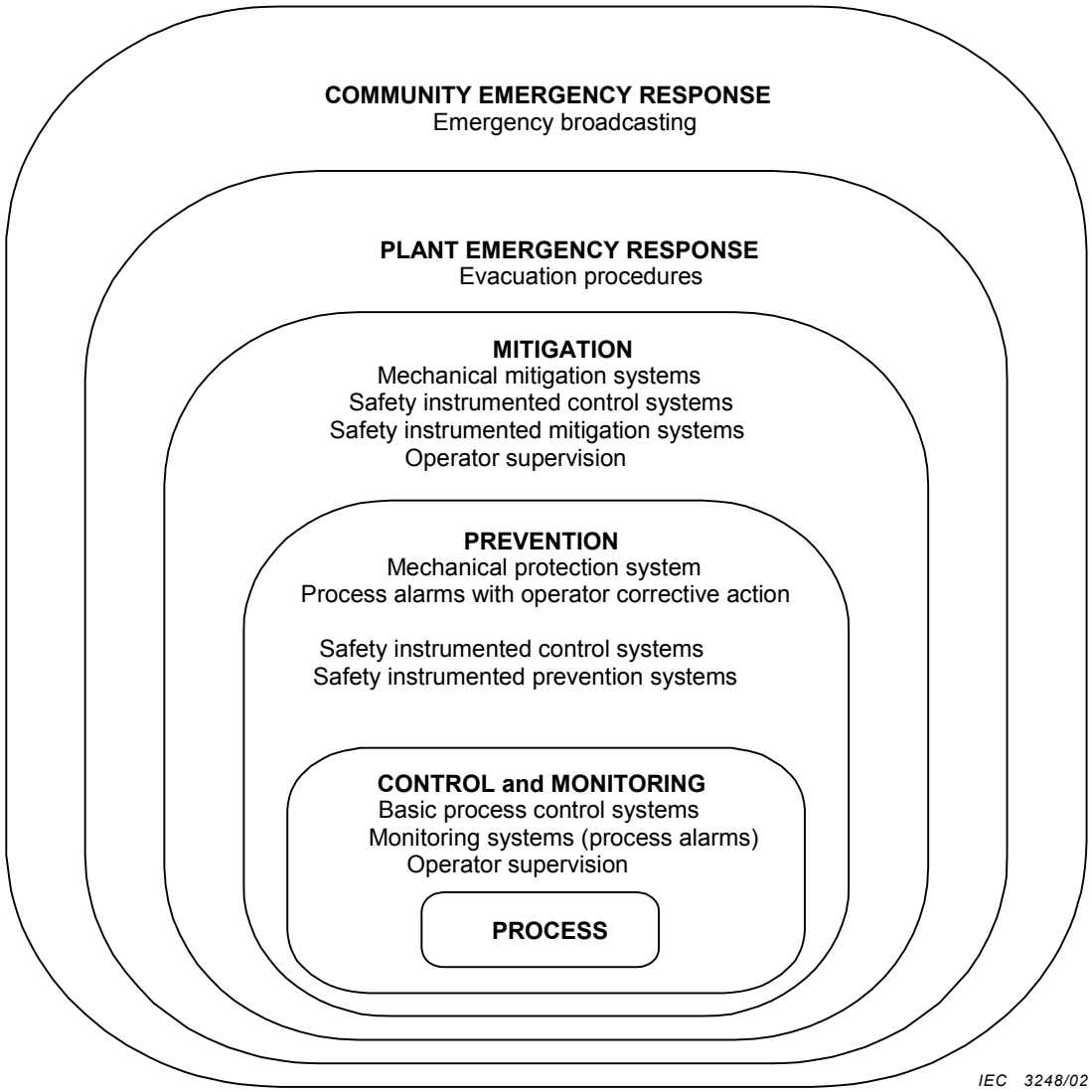


Figure 9 – Typical risk reduction methods found in process plants

9.4.2 The risk reduction factor for a BPCS (which does not conform to IEC 61511 or IEC 61508) used as a protection layer shall be below 10.

NOTE When considering how much risk reduction credit to be given to a BPCS, consideration should be given to the fact that a part of the BPCS may also be an initiating source for an event.

9.4.3 If a risk reduction factor greater than 10 is claimed for the BPCS, then it shall be designed to the requirements within this standard.

9.5 Exigences pour prévenir les défaillances de cause commune, les défaillances de mode commun et les défaillances dépendantes

9.5.1 La conception des couches de protection doit être évaluée pour assurer que la vraisemblance des défaillances de cause commune, de mode commun et dépendantes, entre les couches de protection et entre ces dernières et le BPCS, est suffisamment faible par rapport aux exigences globales d'intégrité de sécurité des couches de protection. L'évaluation peut être qualitative ou quantitative.

NOTE Une définition des défaillances dépendantes est donnée en 3.2.12.

9.5.2 L'évaluation doit prendre en compte les points suivants:

- l'indépendance entre les couches de protection;
- la diversité entre les couches de protection;
- la séparation physique entre les différentes couches de protection;
- les défaillances de cause commune entre les couches de protection et entre ces dernières et le BPCS (par exemple, l'obstruction de soupapes de sécurité d'un réservoir provoque les mêmes problèmes que l'obturation de capteurs dans un SIS).

10 Spécification des exigences concernant la sécurité d'un SIS

10.1 Objectif

L'objectif de cet article est de spécifier les exigences relatives à la (aux) fonction(s) instrumentée(s) de sécurité.

10.2 Exigences générales

10.2.1 Les exigences de sécurité doivent résulter de l'allocation des fonctions instrumentées de sécurité et des exigences identifiées lors de la planification de sécurité.

NOTE Il convient que les exigences du SIS soient exprimées et structurées de telle manière qu'elles soient:

– claires, précises, vérifiables, maintenables et réalisables; et

– écrites de manière à aider les personnes susceptibles d'utiliser les informations, à bien les comprendre, à n'importe quelle phase du cycle de vie.

10.3 Exigences concernant la sécurité du SIS

10.3.1 Ces exigences doivent être suffisantes pour concevoir le SIS et doivent inclure les points suivants:

- une description de toutes les fonctions instrumentées de sécurité nécessaires pour obtenir la sécurité fonctionnelle requise;
- les exigences pour identifier et tenir compte des défaillances de cause commune;
- une définition de l'état de sécurité du processus pour chaque fonction instrumentée de sécurité identifiée;
- une définition de tous les états du processus, individuellement sûrs, qui, en ayant lieu concurremment, créent un danger distinct (par exemple, surcharge de stockage d'urgence, dégazage multiple par système à torche);
- les sources supposées de sollicitation et le taux de sollicitation relatifs à la fonction instrumentée de sécurité;
- les exigences pour les intervalles de tests périodiques;
- les exigences de temps de réponse pour que le SIS conduise le processus à un état de sécurité;

9.5 Requirements for preventing common cause, common mode and dependent failures

9.5.1 The design of the protection layers shall be assessed to ensure that the likelihood of common cause, common mode and dependent failures between protection layers and between protection layers and the BPCS are sufficiently low in comparison to the overall safety integrity requirements of the protection layers. The assessment may be qualitative or quantitative.

NOTE For a definition of dependent failure, see 3.2.12.

9.5.2 The assessment shall consider the following:

- independency between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS (for example, can plugging of relief valves cause the same problems as plugging of sensors in a SIS?).

10 SIS safety requirements specification

10.1 Objective

The objective of this clause is to specify the requirements for the safety instrumented function(s).

10.2 General requirements

10.2.1 The safety requirements shall be derived from the allocation of safety instrumented functions and from those requirements identified during safety planning.

NOTE The SIS requirements should be expressed and structured in such a way that they are

– clear, precise, verifiable, maintainable and feasible; and

– written to aid comprehension by those who are likely to utilize the information at any phase of the life cycle.

10.3 SIS safety requirements

10.3.1 These requirements shall be sufficient to design the SIS and shall include the following:

- a description of all the safety instrumented functions necessary to achieve the required functional safety;
- requirements to identify and take account of common cause failures;
- a definition of the safe state of the process for each identified safety instrumented function;
- a definition of any individually safe process states which, when occurring concurrently, create a separate hazard (for example, overload of emergency storage, multiple relief to flare system);
- the assumed sources of demand and demand rate on the safety instrumented function;
- requirement for proof-test intervals;
- response time requirements for the SIS to bring the process to a safe state;

- le niveau d'intégrité de sécurité et le mode de fonctionnement (sollicitation/continu) pour chaque fonction instrumentée de sécurité;
- une description des mesures du processus du SIS et de leurs points de déclenchement;
- une description des actions de sortie du processus du SIS et des critères de bon fonctionnement, par exemple, exigences pour des vannes à faible coefficient de fuite;
- les relations fonctionnelles entre les entrées et les sorties du processus, y compris les fonctions logiques, mathématiques et tous les acquittements requis;
- les exigences pour l'arrêt manuel;
- les exigences relatives à l'excitation ou à la désexcitation au déclenchement;
- les exigences pour réinitialiser le SIS après un arrêt;
- le taux de déclenchement parasite permis maximal;
- les modes de défaillance et la réponse désirée du SIS (par exemple, alarmes, arrêt automatique);
- toutes les exigences spécifiques relatives aux procédures de démarrage et de redémarrage du SIS;
- toutes les interfaces entre le SIS et tout autre système (y compris le BPCS et les opérateurs);
- une description du mode de fonctionnement de l'installation industrielle et l'identification des fonctions instrumentées de sécurité requises, pour fonctionner dans chaque mode;
- les exigences de sécurité du logiciel d'application comme cela est listé en 12.2.2;
- les exigences concernant les annulations prioritaires/les inhibitions/les dérivations, comprenant la façon dont elles seront désactivées;
- les spécifications de toute action nécessaire pour obtenir ou maintenir un état de sécurité en cas de défaut(s) détectés dans le SIS. Cette action doit être déterminée en tenant compte de tous les facteurs humains pertinents;
- le temps moyen de réparation qui est réalisable pour le SIS, en tenant compte du temps du déplacement, du lieu, du stock de pièces de rechange, des contrats d'entretien, des contraintes environnementales;
- l'identification des combinaisons dangereuses des états de sortie du SIS, qui doivent être évitées;
- les valeurs extrêmes de toutes les conditions environnementales, qui sont susceptibles d'être rencontrées par le SIS, doivent être identifiées. Ceci peut nécessiter de prendre en compte les points suivants: la température, l'humidité, les contaminants, la mise à la terre, les interférences électromagnétiques/les interférences radiofréquence (IEM/IRF), les chocs/ vibrations, les décharges électrostatiques, la classification en zones électriques, la submersion, la foudre, et tout autre facteur pertinent;
- l'identification des modes normaux et anormaux pour les procédures opérationnelles, à la fois de l'installation industrielle dans son ensemble (par exemple: mise en route de l'installation) et de l'installation individuelle (par exemple: maintenance des équipements, étalonnage d'un capteur et/ou réparation). Des fonctions instrumentées de sécurité supplémentaires peuvent être requises pour supporter ces modes de fonctionnement;
- la définition des exigences pour toute fonction instrumentée de sécurité nécessaire pour survivre à un événement accidentel majeur, par exemple, temps requis pendant lequel une vanne reste opérationnelle en cas d'incendie.

NOTE Des fonctions instrumentées non sécuritaires peuvent être exécutées par le SIS pour assurer un arrêt normal ou un démarrage plus rapide. Il convient que celles-ci soient distinctes des fonctions instrumentées de sécurité.

10.3.2 Les spécifications des exigences concernant la sécurité du logiciel doivent résulter des spécifications des exigences concernant la sécurité et de l'architecture choisie pour le SIS.

- the safety integrity level and mode of operation (demand/continuous) for each safety instrumented function;
- a description of SIS process measurements and their trip points;
- a description of SIS process output actions and the criteria for successful operation, for example, requirements for tight shut-off valves;
- the functional relationship between process inputs and outputs, including logic, mathematical functions and any required permissives;
- requirements for manual shutdown;
- requirements relating to energize or de-energize to trip;
- requirements for resetting the SIS after a shutdown;
- maximum allowable spurious trip rate;
- failure modes and desired response of the SIS (for example, alarms, automatic shut-down);
- any specific requirements related to the procedures for starting up and restarting the SIS;
- all interfaces between the SIS and any other system (including the BPCS and operators);
- a description of the modes of operation of the plant and identification of the safety instrumented functions required to operate within each mode;
- the application software safety requirements as listed in 12.2.2;
- requirements for overrides/inhibits/bypasses including how they will be cleared;
- the specification of any action necessary to achieve or maintain a safe state in the event of fault(s) being detected in the SIS. Any such action shall be determined taking account of all relevant human factors;
- the mean time to repair which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints;
- identification of the dangerous combinations of output states of the SIS that need to be avoided;
- the extremes of all environmental conditions that are likely to be encountered by the SIS shall be identified. This may require consideration of the following: temperature, humidity, contaminants, grounding, electromagnetic interference/radiofrequency interference (EMI/RFI), shock/vibration, electrostatic discharge, electrical area classification, flooding, lightning, and other related factors;
- identification to normal and abnormal modes for both the plant as a whole (for example, plant start-up) and individual plant operational procedures (for example, equipment maintenance, sensor calibration and/or repair). Additional safety instrumented functions may be required to support these modes of operation;
- definition of the requirements for any safety instrumented function necessary to survive a major accident event, for example, time required for a valve to remain operational in the event of a fire.

NOTE Non-safety instrumented functions may be carried out by the SIS to ensure orderly shutdown or faster start-up. These should be separated from the safety instrumented functions.

10.3.2 The software safety requirements specification shall be derived from the safety requirements specification and the chosen architecture of the SIS.

11 Conception et ingénierie du SIS

11.1 Objectif

L'objectif des exigences de cet article est de concevoir un ou plusieurs SIS destinés à pourvoir à la (aux) fonction(s) instrumentée(s) de sécurité et à satisfaire au(x) niveau(x) spécifié(s) d'intégrité de sécurité.

11.2 Exigences générales

11.2.1 La conception du SIS doit être conforme aux spécifications des exigences concernant la sécurité du SIS, et tenir compte de toutes les exigences de cet article.

11.2.2 Dans les cas où le SIS doit mettre en œuvre à la fois une (des) fonction(s) instrumentée(s) de sécurité et une (des) fonction(s) instrumentée(s) non sécuritaire(s), tous les matériels et les logiciels qui peuvent affecter de manière néfaste une SIF quelconque, dans des conditions normales et dans des conditions défectueuses, doivent être traités en tant qu'élément du SIS et être conformes aux exigences relatives au plus haut SIL.

NOTE 1 Dans tous les cas où cela est réalisable, il convient que les fonctions instrumentées de sécurité soient distinctes des fonctions instrumentées non sécuritaires.

NOTE 2 Une indépendance adéquate (fonctions distinctes) signifie que ni une défaillance d'une fonction quelconque non sécuritaire, ni l'accès à la programmation des fonctions logicielles non sécuritaires, ne sont capables de provoquer une défaillance dangereuse des fonctions instrumentées de sécurité.

11.2.3 Dans les cas où le SIS doit mettre en œuvre des fonctions instrumentées de sécurité de différents niveaux d'intégrité de sécurité, les matériels et les logiciels partagés ou communs doivent être conformes au plus haut niveau d'intégrité de sécurité, à moins qu'il puisse être démontré que les fonctions instrumentées de sécurité de niveau d'intégrité de sécurité plus faible ne peuvent pas affecter de manière néfaste les fonctions instrumentées de sécurité de niveaux d'intégrité de sécurité supérieurs.

11.2.4 S'il est prévu de ne pas qualifier le système de commande de processus de base par rapport à cette norme, ce dernier doit être conçu pour être distinct et indépendant, de telle sorte que l'intégrité fonctionnelle du système instrumenté de sécurité n'est pas compromise.

NOTE 1 Des informations de fonctionnement peuvent être échangées, mais il convient qu'elles ne compromettent pas la sécurité fonctionnelle du SIS.

NOTE 2 Des dispositifs du SIS peuvent également être utilisés pour des fonctions du système de commande de processus de base, s'il peut être démontré qu'une défaillance du système de commande de processus de base ne compromet pas les fonctions instrumentées de sécurité du système instrumenté de sécurité.

11.2.5 Les exigences concernant l'aptitude à l'exploitation, à la maintenance et à aux essais doivent être prises en compte lors de la conception du SIS afin de faciliter la mise en oeuvre des exigences relatives à l'ergonomie dès la conception (par exemple, dispositifs de dérivation pour permettre les essais et l'alarme en ligne, sous dérivation).

NOTE Il convient que les dispositifs de maintenance et d'essai soient conçus pour réduire autant que faire se peut l'éventualité de défaillances dangereuses résultant de leur utilisation.

11.2.6 La conception du SIS doit tenir compte des possibilités et des limites humaines et être adaptée aux tâches assignées aux opérateurs et au personnel de maintenance. La conception de toutes les interfaces homme-machine doit suivre la bonne pratique ergonomique et doit être adaptée au niveau probable de formation ou de sensibilisation que les opérateurs devraient recevoir.

11.2.7 Le SIS doit être conçu de telle sorte qu'après avoir placé le processus dans un état de sécurité, il doit rester dans cet état jusqu'à ce qu'une réinitialisation soit lancée, sauf indication contraire donnée par les spécifications des exigences concernant la sécurité.

11 SIS design and engineering

11.1 Objective

The objective of the requirements of this clause is to design one or multiple SIS to provide the safety instrumented function(s) and meet the specified safety integrity level(s).

11.2 General requirements

11.2.1 The design of the SIS shall be in accordance with the SIS safety requirements specifications, taking into account all the requirements of this clause.

11.2.2 Where the SIS is to implement both safety and non-safety instrumented function(s) then all the hardware and software that can negatively affect any SIF under normal and fault conditions shall be treated as part of the SIS and comply with the requirements for the highest SIL.

NOTE 1 Wherever practicable, the safety instrumented functions should be separated from the non-safety instrumented functions.

NOTE 2 Adequate independence means that neither the failure of any non-safety functions nor the programming access to the non-safety software functions is capable of causing a dangerous failure of the safety instrumented functions.

11.2.3 Where the SIS is to implement safety instrumented functions of different safety integrity levels, then the shared or common hardware and software shall conform to the highest safety integrity level unless it can be shown that the safety instrumented functions of lower safety integrity level cannot negatively affect the safety instrumented functions of higher safety integrity levels.

11.2.4 If it is intended not to qualify the basic process control system to this standard, then the basic process control system shall be designed to be separate and independent to the extent that the functional integrity of the safety instrumented system is not compromised.

NOTE 1 Operating information may be exchanged but should not compromise the functional safety of the SIS.

NOTE 2 Devices of the SIS may also be used for functions of the basic process control system if it can be shown that a failure of the basic process control system does not compromise the safety instrumented functions of the safety instrumented system.

11.2.5 Requirements for operability, maintainability and testability shall be addressed during the design of the SIS in order to facilitate implementation of human factor requirements in the design (for example, by-pass facilities to allow on-line testing and alarm when in bypass).

NOTE The maintenance and test facilities should be designed to minimize as far as practicable the likelihood of dangerous failures arising from their use.

11.2.6 The design of the SIS shall take into account human capabilities and limitations and be suitable for the task assigned to operators and maintenance staff. The design of all human-machine interfaces shall follow good human factors practice and shall accommodate the likely level of training or awareness that operators should receive.

11.2.7 The SIS shall be designed in such a way that once it has placed the process in a safe state, it shall remain in the safe state until a reset has been initiated unless otherwise directed by the safety requirement specifications.

11.2.8 Des moyens manuels (par exemple, bouton poussoir d'arrêt d'urgence), indépendants de l'unité logique, doivent être mis à disposition pour actionner les éléments terminaux du SIS, sauf indication contraire donnée par les spécifications des exigences concernant la sécurité.

11.2.9 La conception du SIS doit prendre en considération tous les aspects de l'indépendance et de la dépendance entre le SIS et le BPCS, et entre le SIS et les autres couches de protection.

11.2.10 A moins qu'une analyse ait été effectuée pour confirmer que le risque global est acceptable, un dispositif utilisé pour exécuter une partie d'une fonction instrumentée de sécurité ne doit pas être utilisé pour la commande de processus de base, là où une défaillance de ce dispositif aurait pour conséquence une défaillance de la fonction de commande de processus de base, laquelle provoquerait une sollicitation sur la fonction instrumentée de sécurité.

NOTE Lorsqu'une partie du SIS est également utilisée dans un but de commande et qu'une défaillance dangereuse des équipements communs peut provoquer une sollicitation de la fonction exécutée par le SIS, un nouveau risque peut être introduit. Le risque supplémentaire dépend du taux des défaillances dangereuses du composant partagé, du fait que, si le composant partagé tombe en panne, une sollicitation sera créée immédiatement, à la laquelle le SIS peut ne pas être capable de répondre. Pour cette raison, l'analyse supplémentaire sera nécessaire dans ces cas, pour assurer que le taux des défaillances dangereuses des équipements partagés est suffisamment bas. Les capteurs et les vannes sont des exemples où le partage des équipements avec le BPCS est souvent pris en compte.

11.2.11 Pour les sous-systèmes, qui sur une perte de puissance, ne remettent pas en cause l'état de sécurité, toutes les exigences suivantes doivent être satisfaites et une action doit être prise en accord avec 11.3:

- la perte d'intégrité de circuit est détectée (par exemple, surveillance de bout de ligne);
- l'intégrité de l'alimentation en énergie est assurée, en utilisant une alimentation auxiliaire (par exemple, batterie de secours, alimentations sans coupure);
- la perte d'alimentation au niveau du sous-système est détectée.

11.3 Exigences relatives au comportement du système lors de la détection d'une anomalie

11.3.1 La détection d'une anomalie dangereuse (par essais de diagnostic, tests périodiques ou par tout autre moyen) dans un sous-système quelconque pouvant tolérer une anomalie unique de matériel, aura une des deux conséquences ci-après:

a) une action spécifiée pour obtenir ou maintenir un état de sécurité (voir la note); ou

b) la poursuite du fonctionnement du processus en toute sécurité, pendant que la partie défectueuse est réparée. Si la réparation de la partie défectueuse n'est pas terminée dans le temps moyen de rétablissement (MTTR) pris par hypothèse dans le calcul de la probabilité de défaillance aléatoire du matériel, une action spécifiée aura alors lieu pour obtenir ou maintenir un état de sécurité (voir la note).

Dans le cas où les actions ci-dessus dépendent d'un opérateur qui prend des mesures spécifiques en réponse à une alarme (par exemple, ouverture ou fermeture d'une vanne), l'alarme doit être considérée comme faisant partie du système instrumenté de sécurité (c'est-à-dire, indépendante du BPCS).

Dans le cas où les actions ci-dessus dépendent d'un opérateur qui décide d'une opération de maintenance pour réparer un système défectueux en réponse à l'alarme de diagnostic, cette dernière peut faire partie du BPCS, mais doit être soumise aux tests périodiques et à la gestion des modifications appropriés, tout comme le reste du SIS.

11.2.8 Manual means (for example, emergency stop push button), independent of the logic solver, shall be provided to actuate the SIS final elements unless otherwise directed by the safety requirement specifications.

11.2.9 The design of the SIS shall take into consideration all aspects of independence and dependence between the SIS and BPCS, and the SIS and other protection layers.

11.2.10 A device used to perform part of a safety instrumented function shall not be used for basic process control purposes, where a failure of that device results in a failure of the basic process control function which causes a demand on the safety instrumented function, unless an analysis has been carried out to confirm that the overall risk is acceptable.

NOTE When a part of the SIS is also used for control purposes and a dangerous failure of the common equipment would cause a demand for the function performed by the SIS, then a new risk is introduced. The additional risk is dependent on the dangerous failure rate of the shared component because if the shared component fails, a demand will be created immediately to which the SIS may not be capable of responding . For that reason, additional analysis will be necessary in these cases to ensure that the dangerous failure rate of the shared equipment is sufficiently low. Sensors and valves are examples where sharing of equipment with the BPCS is often considered.

11.2.11 For subsystems that on loss of power do not fail to the safe state, all of the following requirements shall be met and action taken according to 11.3:

- loss of circuit integrity is detected (for example, end-of-line monitoring);
- power supply integrity is ensured using supplemental power supply (for example, battery back-up, uninterruptible power supplies);
- loss of power to the subsystem is detected.

11.3 Requirements for system behaviour on detection of a fault

11.3.1 The detection of a dangerous fault (by diagnostic tests, proof tests or by any other means) in any subsystem which can tolerate a single hardware fault shall result in either

a) a specified action to achieve or maintain a safe state (see note); or

b) continued safe operation of the process whilst the faulty part is repaired. If the repair of the faulty part is not completed within the mean time to restoration (MTTR) assumed in the calculation of the probability of random hardware failure, then a specified action shall take place to achieve or maintain a safe state (see note).

Where the above actions depend on an operator taking specific actions in response to an alarm (for example, opening or closing a valve), then the alarm shall be considered part of the safety instrumented system (i.e., independent of the BPCS).

Where the above actions depend on an operator notifying maintenance to repair a faulty system in response to diagnostic alarm, this diagnostic alarm may be a part of the BPCS but shall be subject to appropriate proof testing and management of change along with the rest of the SIS.

NOTE Il convient que l'action spécifiée (réaction à l'anomalie) requise pour obtenir ou maintenir un état de sécurité soit spécifiée dans les exigences concernant la sécurité (voir 10.3). Elle peut consister, par exemple, en un arrêt de sécurité du processus, ou de la partie du processus qui s'appuie, pour la réduction de risque, sur le sous-système défectueux ou sur toute autre planification spécifiée de l'atténuation.

11.3.2 Dans le cas d'un sous-système qui n'utilise qu'une ou des fonction(s) instrumentée(s) de sécurité fonctionnant en mode de sollicitation, la détection d'une anomalie dangereuse (par essai de diagnostic, tests périodiques ou par tout autre moyen) dans un sous-système quelconque n'ayant aucune redondance et sur lequel une fonction instrumentée de sécurité est entièrement dépendante (voir la note 1) doit avoir une des deux conséquences ci-après:

a) une action spécifiée pour obtenir ou maintenir un état de sécurité; ou

b) la réparation du sous-système défectueux dans la période du temps moyen de rétablissement (MTTR) prise pour hypothèse dans le calcul de la probabilité de défaillance aléatoire du matériel. Pendant ce temps la continuation de la sécurité du processus doit être assurée par des mesures et des contraintes supplémentaires. La réduction de risque apportée par ces mesures et contraintes doit être au moins égale à la réduction de risque apportée par le système instrumenté de sécurité, en l'absence d'anomalie. Les mesures et les contraintes supplémentaires doivent être spécifiées dans les procédures d'exploitation et de maintenance du SIS. Si la réparation n'est pas entreprise dans le temps moyen de rétablissement indiqué (MTTR), une action spécifiée doit alors être effectuée pour obtenir ou maintenir un état de sécurité (voir la note 2).

Dans le cas où les actions ci-dessus dépendent d'un opérateur qui prend des mesures spécifiques en réponse à une alarme (par exemple, ouverture ou fermeture d'une vanne), l'alarme doit être considérée comme faisant partie du système instrumenté de sécurité (c'est-à-dire, indépendante du BPCS).

Dans le cas où les actions ci-dessus dépendent d'un opérateur qui décide d'une opération de maintenance pour réparer un système défectueux en réponse à l'alarme de diagnostic, cette dernière peut faire partie du BPCS, mais doit être soumise aux tests périodiques et à la gestion des modifications appropriés, tout comme le reste du SIS.

NOTE 1 Une fonction instrumentée de sécurité est considérée comme entièrement dépendante d'un sous-système, si une défaillance de ce sous-système a comme conséquence une défaillance de la fonction instrumentée de sécurité dans le système instrumenté de sécurité en question, et si la fonction instrumentée de sécurité n'a pas aussi été allouée à une autre couche de protection (voir l'Article 9).

NOTE 2 Il convient que l'action spécifiée (réaction à l'anomalie) requise pour obtenir ou maintenir un état de sécurité soit spécifiée dans les exigences concernant la sécurité (voir 10.3). Elle peut consister, par exemple, en un arrêt de sécurité du processus, ou de la partie du processus qui s'appuie, pour la réduction de risque, sur le sous-système défectueux ou sur toute autre planification spécifiée de l'atténuation.

11.3.3 La détection d'une anomalie dangereuse (par essai de diagnostic, tests périodiques ou par tout autre moyen) dans un sous-système quelconque n'ayant aucune redondance et sur lequel une fonction instrumentée de sécurité est entièrement dépendante (voir la note 1) doit avoir comme conséquence une action spécifiée pour obtenir ou maintenir un état de sécurité, dans le cas d'un sous-système qui met en oeuvre une ou des fonction(s) instrumentée(s) de sécurité fonctionnant en mode continu.

L'action spécifiée (réaction à l'anomalie) requise pour obtenir ou maintenir un état de sécurité doit être spécifiée dans les exigences concernant la sécurité. Elle peut consister, par exemple, en un arrêt de sécurité du processus, ou de la partie du processus qui s'appuie, pour la réduction de risque, sur le sous-système défectueux ou sur toute autre planification spécifiée de l'atténuation. Le temps total pour détecter l'anomalie et pour effectuer l'action doit être inférieur au temps d'apparition de l'événement dangereux.

Dans le cas où les actions ci-dessus dépendent d'un opérateur qui prend des mesures spécifiques en réponse à une alarme (par exemple, ouverture ou fermeture d'une vanne), l'alarme doit alors être considérée comme faisant partie du système instrumenté de sécurité (c'est-à-dire, indépendante du BPCS).

NOTE The specified action (fault reaction) required to achieve or maintain a safe state should be specified in the safety requirements (see 10.3). It may consist, for example, of the safe shutdown of the process or of that part of the process which relies, for risk reduction, on the faulty subsystem or other specified mitigation planning.

11.3.2 The detection of a dangerous fault (by diagnostic test, proof tests or by any other means) in any subsystem having no redundancy and on which a safety instrumented function is entirely dependent (see note 1) shall, in the case that the subsystem is used only by safety instrumented function(s) operation in the demand mode, result in either

a) a specified action to achieve or maintain a safe state; or

b) the repair of the faulty subsystem within the mean-time-to-restoration (MTTR) period assumed in the calculation of the probability of random hardware failure. During this time the continuing safety of the process shall be ensured by additional measures and constraints. The risk reduction provided by these measures and constraints shall be at least equal to the risk reduction provided by the safety instrumented system in the absence of any faults. The additional measures and constraints shall be specified in the SIS operation and maintenance procedures. If the repair is not undertaken within the specified mean time to restoration (MTTR) then a specified action shall be performed to achieve or maintain a safe state (see note 2).

Where the above actions depend on an operator taking specific actions in response to an alarm (for example, opening or closing a valve), then the alarm shall be considered part of the safety instrumented system (i.e., independent of the BPCS).

Where the above actions depend on an operator notifying maintenance to repair a faulty system in response to a diagnostic alarm, this diagnostic alarm may be a part of BPCS but shall be subject to appropriate proof testing and management of change along with the rest of the SIS.

NOTE 1 A safety instrumented function is considered to be entirely dependent on a subsystem if a failure of this subsystem results in a failure of the safety instrumented function in the safety instrumented system under consideration, and the safety instrumented function has not also been allocated to another protection layer (see Clause 9).

NOTE 2 The specified action (fault reaction) required to achieve or maintain a safe state should be specified in the safety requirements (see 10.3). It may consist, for example, of the safe shutdown of the process, or that part of the process which relies, for risk reduction, on the faulty subsystem or on other specified mitigation planning.

11.3.3 The detection of a dangerous fault (by diagnostic test, proof tests or by any other means) in any subsystem having no redundancy and on which a safety instrumented function is entirely dependent (see note 1) shall, in the case of a subsystem which is implementing any safety instrumented function(s) operating in the continuous mode (see note 2), result in a specified action to achieve or maintain a safe state.

The specified action (fault reaction) required to achieve or maintain a safe state shall be specified in the safety requirements specification. It may consist, for example, of the safe shutdown of the process, or that part of the process which relies, for risk reduction, on the faulty subsystem, or other specified mitigation planning. The total time to detect the fault and to perform the action shall be less than the time for the hazardous event to occur.

Where the above actions depend on an operator taking specific actions in response to an alarm (for example, opening or closing a valve), then the alarm shall be considered part of the safety instrumented system (i.e., independent of the BPCS).

Dans le cas où les actions ci-dessus dépendent d'un opérateur qui décide d'une opération de maintenance pour réparer un système défectueux en réponse à l'alarme de diagnostic, cette dernière peut faire partie du BPCS, mais doit être soumise aux tests périodiques et à la gestion des modifications appropriés, tout comme le reste du SIS.

NOTE 1 Une fonction instrumentée de sécurité est considérée comme entièrement dépendante d'un sous-système, si une défaillance du sous-système provoque une défaillance de la fonction instrumentée de sécurité dans le système instrumenté de sécurité en question, et si la fonction instrumentée de sécurité n'a pas non plus été allouée à une autre couche de protection.

NOTE 2 Lorsqu'une certaine combinaison des états de sortie d'un sous-système a la possibilité de provoquer directement un événement dangereux, il convient alors de considérer nécessairement la détection des anomalies dangereuses dans le sous-système comme une fonction instrumentée de sécurité fonctionnant en régime continu.

11.4 Exigences relatives à la tolérance aux anomalies du matériel

11.4.1 Pour les fonctions instrumentées de sécurité, les capteurs, les unités logiques et les éléments terminaux doivent avoir une tolérance aux anomalies du matériel (HFT) minimale.

NOTE 1 La tolérance aux anomalies du matériel est la capacité d'un composant ou d'un sous-système à continuer à être capable d'assumer la fonction instrumentée de sécurité requise en présence d'une ou de plusieurs anomalies dangereuses dans le matériel. Une tolérance aux anomalies du matériel de 1 signifie qu'il y a par exemple deux dispositifs et que l'architecture est telle que la défaillance dangereuse d'un des deux composants ou sous-systèmes n'empêche pas une activité de sécurité d'avoir lieu.

NOTE 2 La tolérance minimale aux anomalies du matériel a été définie pour minimiser des imperfections potentielles de la conception de la SIF, qui peuvent résulter du nombre de suppositions faites lors de cette conception, ainsi que de l'incertitude des taux de défaillance des composants ou des sous-systèmes utilisés dans diverses applications du processus.

NOTE 3 Il est important de noter que les exigences de tolérance aux anomalies du matériel représentent la redondance minimale des composants ou des sous-systèmes. Selon l'application, le taux de défaillance des composants et l'intervalle des tests périodiques, une redondance supplémentaire peut être requise pour satisfaire au SIL de la SIF, en accord avec 11.9.

11.4.2 Pour les unités logiques de l'électronique programmable (PE), la tolérance minimale aux anomalies du matériel doit être celle indiquée par le Tableau 5.

Tableau 5 – Tolérance minimale aux anomalies du matériel pour les unités logiques de l'électronique programmable (PE)

SIL	Tolérance minimale aux anomalies du matériel		
	SFF < 60%	SFF 60% à 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Les exigences spéciales s'appliquent – voir la CEI 61508		

11.4.3 Pour tous les sous-systèmes (par exemple, capteurs, éléments terminaux et unités logiques non-PE), excepté les unités logiques PE, la tolérance minimale aux anomalies du matériel doit être celle indiquée par le Tableau 6, à condition que le mode de défaillance dominant soit à un état de sécurité ou que des défaillances dangereuses soient détectées (voir 11.3), sinon la tolérance aux anomalies doit être augmentée de 1.

NOTE Pour établir si le mode dominant de défaillance est à l'état de sécurité ou non, il est nécessaire de considérer chacun des points suivants:

– la connexion de processus du dispositif;

– l'utilisation des informations de diagnostic du dispositif pour valider le signal de processus;

– l'utilisation du comportement à sécurité intrinsèque inhérent au dispositif (par exemple, absence de signal actif, perte d'alimentation entraînant un état de sécurité).

Where the above actions depend on an operator notifying maintenance to repair a faulty system in response to a diagnostic alarm, this diagnostic alarm may be a part of the BPCS but shall be subject to appropriate proof testing and management of change along with the rest of the SIS.

NOTE 1 A safety instrumented function is considered to be entirely dependent on a subsystem if a failure of the subsystem causes a failure of the safety instrumented function in the safety instrumented system under consideration, and the safety instrumented function has not also been allocated to another protection layer.

NOTE 2 When there is a possibility that some combination of output states of a subsystem can directly cause a hazardous event then it should be necessary to regard the detection of dangerous faults in the subsystem as a safety instrumented function operating in the continuous mode.

11.4 Requirements for hardware fault tolerance

11.4.1 For safety instrumented functions, the sensors, logic solvers and final elements shall have a minimum hardware fault tolerance.

NOTE 1 Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring.

NOTE 2 The minimum hardware fault tolerance has been defined to alleviate potential shortcomings in SIF design that may result due to the number of assumptions made in the design of the SIF, along with uncertainty in the failure rate of components or subsystems used in various process applications.

NOTE 3 It is important to note that the hardware fault tolerance requirements represent the minimum component or subsystem redundancy. Depending on the application, component failure rate and proof-testing interval, additional redundancy may be required to satisfy the SIL of the SIF according to 11.9.

11.4.2 For PE logic solvers, the minimum hardware fault tolerance shall be as shown in Table 5.

Table 5 – Minimum hardware fault tolerance of PE logic solvers

SIL	Minimum hardware fault tolerance		
	SFF < 60 %	SFF 60 % to 90 %	SFF > 90 %
1	1	0	0
2	2	1	0
3	3	2	1
4	Special requirements apply (see IEC 61508)		

11.4.3 For all subsystems (for example, sensors, final elements and non-PE logic solvers) except PE logic solvers the minimum hardware fault tolerance shall be as shown in Table 6 provided that the dominant failure mode is to the safe state or dangerous failures are detected (see 11.3), otherwise the fault tolerance shall be increased by one.

NOTE To establish whether the dominant failure mode is to the safe state it is necessary to consider each of the following:

- the process connection of the device;
- use of diagnostic information of the device to validate the process signal;
- use of inherent fail safe behaviour of the device (for example, live zero signal, loss of power results in a safe state).

11.4.4 Pour tous les sous-systèmes (par exemple, capteurs, éléments terminaux et unités logiques non-PE), excepté les unités logiques PE, la tolérance minimale aux anomalies spécifiée dans le Tableau 6 peut être réduite de 1, si les dispositifs utilisés satisfont à tous les points suivants:

- le matériel du dispositif est choisi sur la base d'une utilisation antérieure (voir 11.5.3);
- le dispositif ne permet que le réglage des paramètres relatifs au processus, par exemple, gamme de mesure, sens de la défaillance, montant ou descendant;
- le réglage des paramètres relatifs au processus du dispositif est protégé, par exemple, cavalier, mot de passe;
- la fonction a une prescription de SIL inférieure à 4 .

Tableau 6 – Tolérance minimale aux anomalies du matériel pour les capteurs, les éléments terminaux et les unités logiques non-PE

SIL	Tolérance minimale aux anomalies du matériel (voir 11.4.3 et 11.4.4)
1	0
2	1
3	2
4	Les exigences spéciales s'appliquent – voir la CEI 61508

11.4.5 D'autres exigences de tolérance aux anomalies peuvent être utilisées pourvu qu'une évaluation soit faite en accord avec les exigences de la CEI 61508-2, Tableaux 2 et 3.

11.5 Exigences relatives au choix des composants et des sous-systèmes

11.5.1 Objectifs

11.5.1.1 Le premier objectif de ce paragraphe est de spécifier les exigences pour le choix des composants ou des sous-systèmes qui doivent être utilisés en tant qu'élément d'un système instrumenté de sécurité.

11.5.1.2 Le deuxième objectif de ce paragraphe est de spécifier les exigences pour permettre à un composant ou à un sous-système d'être intégré dans l'architecture d'un SIS.

11.5.1.3 Le troisième objectif de ce paragraphe est de spécifier des critères d'acceptation pour les composants et les sous-systèmes en termes de fonctions instrumentées de sécurité associées et d'intégrité de sécurité.

11.5.2 Exigences générales

11.5.2.1 Les composants et les sous-systèmes choisis pour être utilisés en tant qu'éléments d'un système instrumenté de sécurité pour des applications de SIL 1 à SIL 3 doivent, soit être conformes à la CEI 61508-2 et à la CEI 61508-3, suivant les cas, soit être conforme à 11.4 et 11.5.3 à 11.5.6, selon le cas.

11.5.2.2 Les composants et les sous-systèmes choisis pour être utilisés en tant qu'éléments d'un système instrumenté de sécurité pour des applications de SIL 4 doivent être conformes à la CEI 61508-2 et à la CEI 61508-3, selon le cas.

11.4.4 For all subsystems (for example, sensor, final elements and non-PE logic solvers) excluding PE logic solvers the minimum fault tolerance specified in Table 6 may be reduced by one if the devices used comply with all of the following:

- the hardware of the device is selected on the basis of prior use (see 11.5.3);
- the device allows adjustment of process-related parameters only, for example, measuring range, upscale or downscale failure direction;
- the adjustment of the process-related parameters of the device is protected, for example, jumper, password;
- the function has an SIL requirement of less than 4.

Table 6 – Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers

SIL	Minimum hardware fault tolerance (see 11.4.3 and 11.4.4)
1	0
2	1
3	2
4	Special requirements apply (see IEC 61508)

11.4.5 Alternative fault tolerance requirements may be used providing an assessment is made in accordance to the requirements of IEC 61508-2, Tables 2 and 3.

11.5 Requirements for selection of components and subsystems

11.5.1 Objectives

11.5.1.1 The first objective of the requirements of this clause is to specify the requirements for the selection of components or subsystems which are to be used as part of a safety instrumented system.

11.5.1.2 The second objective of the requirements of this clause is to specify the requirements to enable a component or subsystem to be integrated in the architecture of a SIS.

11.5.1.3 The third objective of the requirements of this clause is to specify acceptance criteria for components and subsystems in terms of associated safety instrumented functions and safety integrity.

11.5.2 General requirements

11.5.2.1 Components and subsystems selected for use as part of a safety instrumented system for SIL 1 to SIL 3 applications shall either be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate, or else they shall be in accordance with 11.4 and 11.5.3 to 11.5.6, as appropriate.

11.5.2.2 Components and subsystems selected for use as part of a safety instrumented system for SIL 4 applications shall be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate.

11.5.2.3 L'aptitude des composants et des sous-systèmes choisis doit être démontrée, en considérant:

- la documentation pour le matériel et la documentation du logiciel intégré du constructeur;
- si cela est applicable, le choix d'un langage d'application et d'outils appropriés (voir 12.4.4).

11.5.2.4 Les composants et les sous-systèmes doivent être cohérents avec les spécifications des exigences concernant la sécurité du SIS.

NOTE Pour ce qui concerne le choix des composants et des sous-systèmes, tous les autres aspects applicables de cette norme continuent de s'appliquer, y compris les contraintes architecturales, l'intégrité du matériel, le comportement à la détection d'une anomalie et le logiciel d'application.

11.5.3 Exigences relatives au choix des composants et des sous-systèmes basés sur une utilisation antérieure

11.5.3.1 Une preuve pertinente doit être disponible montrant que les composants et les sous-systèmes sont aptes à être utilisés dans le système instrumenté de sécurité.

NOTE 1 Dans le cas d'éléments sur le terrain, il peut exister une importante expérience d'exploitation des applications de sécurité ou non sécuritaires. Ceci peut être utilisé comme base pour la justification.

NOTE 2 Il convient que le niveau de détails de la preuve soit en rapport avec la complexité du composant ou du sous-système considéré et avec la probabilité de défaillance nécessaire pour atteindre le niveau d'intégrité de sécurité requis de la (des) fonction(s) instrumentée(s) de sécurité.

11.5.3.2 La preuve d'aptitude doit comprendre les points suivants:

- la prise en considération des systèmes de qualité, de gestion de personnel et de gestion de configuration du constructeur;
- l'identification et la spécification ad hoc des composants ou des sous-systèmes;
- la démonstration des performances des composants ou des sous-systèmes utilisés avec des profils opérationnels et sous des environnements physiques similaires;

  NOTE Dans le cas des dispositifs de terrain (par exemple, des capteurs et des éléments terminaux) remplissant une fonction donnée, cette fonction est habituellement identique dans les applications de sécurité et dans les applications non sécuritaires, ce qui signifie que le dispositif aura des performances similaires dans les deux types d'applications. Par conséquent, il convient aussi de prendre en considération les performances de ces dispositifs dans les applications non sécuritaires, pour satisfaire à cette prescription.

- l'importance de l'expérience opérationnelle.

  NOTE Pour des dispositifs de terrain, les informations concernant l'expérience opérationnelle sont principalement consignées dans les listes dressées par les utilisateurs d'équipements approuvés pour être utilisés dans leurs installations; elles sont basées sur un historique étendu de bon fonctionnement dans des applications de sécurité et dans des applications non sécuritaires, et sur l'élimination des équipements ne donnant pas entière satisfaction. La liste des dispositifs de terrain peut être utilisée pour appuyer des requêtes d'expérience en exploitation, à condition que:

  – la liste soit mise à jour et revue régulièrement;
  – les dispositifs de terrain ne soient ajoutés que lorsqu'une expérience suffisante en exploitation a été acquise;
  – les dispositifs de terrain soient retirés lorsqu'ils présentent un historique de fonctionnement non satisfaisant;
  – l'application de processus est incluse dans la liste, si cela est pertinent.

11.5.2.3 The suitability of the selected components and subsystems shall be demonstrated through consideration of

- manufacturer hardware and embedded software documentation;
- if applicable, appropriate application language and tool selection (see 12.4.4).

11.5.2.4 The components and subsystems shall be consistent with the SIS safety requirements specifications.

NOTE For the selection of components and subsystems, all the other applicable aspects of this standard still apply, including architectural constraints, hardware integrity, behaviour on detection of a fault and application software.

11.5.3 Requirements for the selection of components and subsystems based on prior use

11.5.3.1 Appropriate evidence shall be available that the components and subsystems are suitable for use in the safety instrumented system.

NOTE 1 In the case of field elements, there may be extensive operating experience either in safety or non-safety applications. This can be used as a basis for the evidence.

NOTE 2 The level of details of the evidence should be in accordance with the complexity of the considered component or subsystem and with the probability of failure necessary to achieve the required safety integrity level of the safety instrumented function(s).

11.5.3.2 The evidence of suitability shall include the following:

- consideration of the manufacturer's quality, management and configuration management systems;
- adequate identification and specification of the components or subsystems;
- demonstration of the performance of the components or subsystems in similar operating profiles and physical environments;

  NOTE In the case of field devices (for example, sensors and final elements) fulfilling a given function, this function is usually identical in safety and non-safety applications, which means that the device will be performing in a similar way in both type of applications. Therefore, consideration of the performance of such devices in non-safety applications should also be deemed to satisfy this requirement.

- the volume of the operating experience.

  NOTE For field devices, information relating to operating experience is mainly recorded in the user's list of equipment approved for use in their facilities, based on an extensive history of successful performance in safety and non-safety applications, and on the elimination of equipment not performing in a satisfactory manner. The list of field devices may be used to support claims of experience in operation, provided that

  – the list is updated and monitored regularly;
  – field devices are only added when sufficient operating experience has been obtained;
  – field devices are removed when they show a history of not performing in a satisfactory manner;
  – the process application is included in the list where relevant.

11.5.4 Exigences relatives au choix des composants programmables FPL et des sous-systèmes (par exemple, dispositifs de terrain) basés sur une utilisation antérieure

11.5.4.1 Les exigences de 11.5.2 et 11.5.3 s'appliquent.

11.5.4.2 Les caractéristiques inutilisées des composants et des sous-systèmes doivent être identifiées en justifiant leur inutilité, et il doit être établi qu'elles sont peu susceptibles de compromettre les fonctions instrumentées de sécurité prescrites.

11.5.4.3 Pour une configuration spécifique et le profil opérationnel du matériel et du logiciel, la justification d'aptitude doit considérer:

- les caractéristique des signaux d'entrée et de sortie;
- les modes d'utilisation;
- les fonctions et les configurations utilisées;
- une utilisation antérieure pour des applications et dans des environnements physiques similaires.

11.5.4.4 Pour les applications de SIL 3, une évaluation formelle (selon 5.2.6.1) du dispositif de FPL doit être effectuée pour montrer que:

- le dispositif de FPL est apte à exécuter d'une part les fonctions prescrites et d'autre part les précédentes utilisations ont montré qu'il y a une assez faible probabilité qu'il ne puisse pas exécuter ces fonctions, d'une manière qui pourrait conduire à un événement dangereux du fait de défaillances aléatoires du matériel ou d'anomalies systématiques du matériel ou du logiciel alors qu'il est utilisé comme un élément du système instrumenté de sécurité;
- les normes appropriées pour le matériel et le logiciel ont été appliquées;
- le dispositif de FPL a été utilisé ou essayé dans des configurations représentatives des profils opérationnels prévus.

11.5.4.5 Pour les applications de SIL 3, un manuel de sécurité comprenant les contraintes d'exploitation, de maintenance et de détection d'anomalies, doit être disponible, en couvrant les configurations typiques du dispositif de FPL et les profils opérationnels prévus.

11.5.5 Exigences relatives au choix des composants programmables LVL et des sous-systèmes (par exemple, unités logiques) basés sur une utilisation antérieure

11.5.5.1 Les exigences suivantes ne peuvent être appliquées qu'aux unités logiques de PE utilisées dans les systèmes instrumentés de sécurité qui mettent en oeuvre des fonctions instrumentées de sécurité de SIL 1 ou de SIL 2.

11.5.5.2 Les exigences de 11.5.4 s'appliquent.

11.5.5.3 Il se peut que des différences entre les profils opérationnels et les environnements physiques d'un composant ou d'un sous-système soient rencontrées précédemment. Dans le cas où le profil opérationnel et l'environnement physique du composant ou du sous-système sont utilisés dans le système instrumenté de sécurité, toutes ces différences doivent alors être identifiées et il doit y avoir une évaluation basée sur l'analyse et les essais, suivant les cas, pour démontrer que la probabilité des anomalies systématiques est suffisamment faible, lorsque le composant ou le sous-système est utilisé dans le système instrumenté de sécurité.

11.5.4 Requirements for selection of FPL programmable components and subsystems (for example, field devices) based on prior use

11.5.4.1 The requirements of 11.5.2 and 11.5.3 apply.

11.5.4.2 Unused features of the components and subsystems shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required safety instrumented functions.

11.5.4.3 For the specific configuration and operational profile of the hardware and software, the evidence of suitability shall consider

- characteristics of input and output signals;
- modes of use;
- functions and configurations used;
- previous use in similar applications and physical environments.

11.5.4.4 For SIL 3 applications, a formal assessment (in accordance with 5.2.6.1) of the FPL device shall be carried out to show that

- the FPL device is both able to perform the required functions and that the previous use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the safety instrumented system, due to either random hardware failures or systematic faults in hardware or software;
- appropriate standards for hardware and software have been applied;
- the FPL device has been used or tested in configurations representative of the intended operational profiles.

11.5.4.5 For SIL 3 applications, a safety manual including constraints for operation, maintenance and fault detection shall be available covering the typical configurations of the FPL device and the intended operational profiles.

11.5.5 Requirements for the selection of LVL programmable components and subsystems (for example, logic solvers) based on prior use

11.5.5.1 The following requirements may only be applied to PE logic solvers used in safety instrumented systems which implement SIL 1 or SIL 2 safety instrumented functions.

11.5.5.2 The requirements of 11.5.4 apply.

11.5.5.3 Where there is any difference between the operational profiles and physical environments of a component or subsystem as experienced previously, and the operational profile and physical environment of the component or subsystem when used within the safety instrumented system, then any such differences shall be identified and there shall be an assessment based on analysis and testing, as appropriate, to show that the likelihood of systematic faults when used in the safety instrumented system is sufficiently low.

11.5.5.4 L'expérience opérationnelle, considérée comme étant nécessaire pour justifier l'aptitude, doit être déterminée en tenant compte:

- du SIL de la fonction instrumentée de sécurité;
- de la complexité et de la fonctionnalité du composant ou du sous-système.

NOTE Voir la CEI 61511-2 qui donne des indications supplémentaires.

11.5.5.5 Pour des applications de SIL 1 ou 2, une unité logique de PE configurée pour la sécurité peut être utilisée, à condition que toutes les dispositions complémentaires suivantes soient satisfaites:

- compréhension des modes de défaillance dangereux;
- utilisation de techniques de configuration de la sécurité qui prennent en compte des modes de défaillance identifiés;
- logiciel intégré faisant preuve, en utilisation, d'un bon historique pour des applications de sécurité;
- protection contre les modifications non autorisées ou fortuites.

NOTE Une unité logique de PE configurée pour la sécurité est une unité logique de catégorie «électronique programmable pour usage général industriel», spécifiquement configurée pour être utilisée dans des applications de sécurité.

11.5.5.6 Une évaluation formelle (selon 5.2.6.1) de toute unité logique de PE, utilisée dans une application de SIL 2, doit être effectuée pour démontrer que:

- d'une part elle est apte à exécuter les fonctions prescrites et d'autre part les précédentes utilisations ont montré qu'il y a une assez faible probabilité pour qu'elle ne puisse pas exécuter ces fonctions, d'une manière qui pourrait conduire à un événement dangereux du fait de défaillances aléatoires du matériel ou d'anomalies systématiques du matériel ou du logiciel, lorsqu'elle est utilisée comme un élément du système instrumenté de sécurité;
- des mesures sont mises en oeuvre pour détecter des anomalies pendant l'exécution du programme et pour lancer la réaction appropriée; ces mesures comprendront tous les points suivants:

– surveillance de la séquence du programme;

– la protection par code contre les modifications ou la détection des défaillances par surveillance en ligne;

– programmation par assertion (technique d'affirmation) des défaillances ou diversité logicielle;

– vérification des limites des variables ou contrôle de la vraisemblance des valeurs;

– approche modulaire.

– les normes de codage appropriées ont été utilisées pour le logiciel intégré et utilitaire;

– elle a été essayée dans des configurations typiques, avec des scénarii d'essai représentatifs des profils opérationnels prévus;

– des modules logiciels et des composants éprouvés/vérifiés ont été utilisés;

– le système a subi une analyse et des essais dynamiques;

– le système n'utilise pas d'intelligence artificielle ni de reconfiguration dynamique;

– les essais d'insertion d'anomalie documentés ont été réalisés.

11.5.5.7 Pour les applications de SIL 2, un manuel de sécurité comprenant les contraintes d'exploitation, de maintenance et de détection d'anomalies, doit être disponible, en couvrant les configurations typiques de l'unité logique de PE et les profils opérationnels prévus.

11.5.5.4 The operating experience considered necessary to justify the suitability shall be determined taking into account

- the SIL of the safety instrumented function;
- the complexity and functionality of the component or subsystem.

NOTE See IEC 61511-2 for further guidance.

11.5.5.5 For SIL 1 or 2 applications, a safety configured PE logic solver may be used provided that all the following additional provisions are met:

- understanding of unsafe failure modes;
- use of techniques for safety configuration that address the identified failure modes;
- the embedded software has a good history of use for safety applications;
- protection against unauthorized or unintended modifications.

NOTE A safety configured PE logic solver is a general purpose industrial grade PE logic solver which is specifically configured for use in safety applications.

11.5.5.6 A formal assessment (in accordance with 5.2.6.1) of any PE logic solver used in a SIL 2 application shall be carried out to show that

- it is both able to perform the required functions and that previous use has shown there is a low enough probability that it will fail in a way which could lead to a hazardous event when used as part of the safety instrumented system, due to either random hardware failures or systematic faults in hardware or software;
- measures are implemented to detect faults during program execution and initiate appropriate reaction; these measures shall comprise all of the following:
  - program sequence monitoring;
  - protection of code against modifications or failure detection by on-line monitoring;
  - failure assertion or diverse programming;
  - range check of variables or plausibility check of values;
  - modular approach;
  - appropriate coding standards have been used for the embedded and utility software;
  - it has been tested in typical configurations, with test cases representative of the intended operational profiles;
  - trusted verified software modules and components have been used;
  - the system has undergone dynamic analysis and testing;
  - the system does not use artificial intelligence nor dynamic reconfiguration;
  - documented fault-insertion testing has been performed.

11.5.5.7 For SIL 2 applications, a safety manual including constraints for operation, maintenance and fault detection shall be available covering the typical configurations of the PE logic solver and the intended operational profiles.

11.5.6 Exigences relatives au choix des composants programmables FVL et des sous-systèmes (par exemple, unités logiques)

11.5.6.1 Lorsque les applications sont programmées en utilisant un FVL, l'unité logique de PE doit être conforme à la CEI 61508-2 et à la CEI 61508-3.

11.6 Dispositifs de terrain

11.6.1 Les dispositifs de terrain doivent être choisis et installés pour réduire au minimum les défaillances qui pourraient résulter d'informations imprécises du fait de circonstances provenant du processus et des conditions environnementales. Les conditions qu'il convient de considérer comprennent: la corrosion, la gélification des matériaux dans les tuyauteries, les solides en suspension, la polymérisation, la cuisson, les températures et pressions extrêmes, la condensation dans les colonnes sèches à action et réaction, et la condensation insuffisante dans les colonnes humides du même type.

11.6.2 L'excitation au déclenchement de circuits d'entrée/sortie discrets doit appliquer une méthode assurant l'intégrité du circuit et de l'alimentation.

NOTE Un exemple d'une telle méthode est un moniteur de bout de ligne, où un courant pilote est continuellement surveillé pour assurer la continuité du circuit et où le courant pilote n'est pas d'amplitude suffisante pour affecter le bon fonctionnement des entrées/sorties.

11.6.3 Chaque dispositif de terrain individuel doit avoir son propre câblage dédié à l'entrée/sortie du système, excepté dans les cas suivants:

- plusieurs capteurs discrets sont connectés en série à une entrée unique et tous les capteurs surveillent le même état du processus (par exemple, surcharges de moteur);
- plusieurs éléments terminaux sont connectés à une sortie unique;

  NOTE Dans le cas de deux vannes connectées à une sortie, ces dernières ont l'obligation de changer d'état en même temps, vis-à-vis de toutes les fonctions instrumentées de sécurité qui utilisent les deux vannes.
- une communication par bus numérique avec des performances de sécurité globales qui satisfont aux exigences d'intégrité du SIF qu'il dessert.

11.6.4 Les capteurs intelligents doivent être protégés en écriture pour prévenir une modification involontaire depuis un site distant, sauf si une revue de sécurité appropriée autorise l'utilisation de la lecture/écriture. Il convient que la revue tienne compte des facteurs humains, tels que le non-respect des procédures.

11.7 Interfaces

Les interfaces homme-machine et les interfaces de communication au SIS peuvent comprendre, mais ne sont pas limitées à:

- la (les) interface(s) opérateur;
- la (les) interface(s) de maintenance/d'ingénierie;
- la (les) interface(s) de communication.

11.7.1 Exigences relatives à l'interface opérateur

11.7.1.1 Lorsque l'interface opérateur du SIS s'effectue par l'intermédiaire de l'interface opérateur du BPCS, il doit être tenu compte des défaillances prévisibles qui peuvent se produire au sein de l'interface opérateur du BPCS.

11.5.6 Requirements for the selection of FVL programmable components and subsystems (for example, logic solvers)

11.5.6.1 When the applications are programmed using a FVL, the PE logic solver shall be in accordance with IEC 61508-2 and IEC 61508-3.

11.6 Field devices

11.6.1 Field devices shall be selected and installed to minimize failures that could result in inaccurate information due to conditions arising from the process and environmental conditions. Conditions that should be considered include corrosion, freezing of materials in pipes, suspended solids, polymerization, cooking, temperature and pressure extremes, condensation in dry-leg impulse lines, and insufficient condensation in wet-leg impulse lines.

11.6.2 Energizing to trip discrete input/output circuits shall apply a method to ensure circuit and power supply integrity.

NOTE An example of such a method is an end-of-line monitor, where a pilot current is continuously monitored to ensure circuit continuity and where the pilot current is not of sufficient magnitude to affect proper I/O operation.

11.6.3 Each individual field device shall have its own dedicated wiring to the system input/output, except in the following cases.

- Multiple discrete sensors are connected in series to a single input and the sensors all monitor the same process condition (for example, motor overloads).
- Multiple final elements are connected to a single output.

  NOTE For two valves connected to one output, both valves are required to change state at the same time for all the safety instrumented functions that use the two valves.
- A digital bus communication with overall safety performance that meets the integrity requirements of the SIF it services.

11.6.4 Smart sensors shall be write-protected to prevent inadvertent modification from a remote location, unless appropriate safety review allows the use of read/write. The review should take into account human factors such as failure to follow procedures.

11.7 Interfaces

Human machine and communication interfaces to the SIS can include, but are not limited to

- operator interface(s);
- maintenance/engineering interface(s);
- communication interface(s).

11.7.1 Operator interface requirements

11.7.1.1 Where the SIS operator interface is via the BPCS operator interface, account shall be taken of credible failures that may occur in the BPCS operator interface.

11.7.1.2 La conception du SIS doit minimiser la nécessité pour l'opérateur de faire des choix d'options et la nécessité de shunter le système, alors que l'unité est en marche. Si la conception exige l'utilisation d'actions de l'opérateur, il convient que cette dernière inclue des fonctions de protection contre les erreurs de l'opérateur.

NOTE Si l'opérateur doit choisir une option particulière, il convient qu'il y ait une étape de répétition pour confirmation.

11.7.1.3 Les commutateurs de dérivation doivent être protégés par des verrouillages à clés ou des mots de passe, pour en empêcher l'utilisation non autorisée.

11.7.1.4 Les informations d'état du SIS, qui sont critiques pour maintenir le SIL, doivent être disponibles, en tant qu'éléments de l'interface opérateur. Ces informations peuvent comprendre:

- où en est le processus dans sa séquence;
- l'indication qu'une action de protection du SIS a eu lieu;
- l'indication qu'une fonction de protection est shuntée;
- l'indication qu'une (des) action(s) automatique(s), comme la dégradation du vote majoritaire et/ou le traitement d'anomalie, a eu lieu;
- l'état des capteurs et des éléments terminaux;
- la perte d'énergie, dans le cas où cette dernière affecte la sécurité;
- les résultats des diagnostics;
- les défaillances des équipements de conditionnement environnemental, qui sont nécessaires pour assister le SIS.

11.7.1.5 La conception de l'interface opérateur du SIS doit être telle qu'elle ne permet pas d'effectuer des modifications au logiciel d'application du SIS. Dans le cas où les informations de sécurité nécessitent d'être transmises du BPCS au SIS, il convient alors d'utiliser des systèmes, qui peuvent sélectivement autoriser l'écriture, depuis le BPCS vers des variables du SIS spécifiques. Il convient que des équipements ou des procédures soient mis en application pour confirmer que le choix correct a été transmis et reçu par le SIS et ne compromet pas la fonctionnalité de sécurité du SIS.

NOTE 1 Si les options ou les dérivations sont choisies dans le BPCS et téléchargées vers le SIS, les défaillances dans le BPCS peuvent interférer avec l'aptitude du SIS à fonctionner sur sollicitation. Si ceci peut se produire, alors le BPCS deviendra (un système) relatif à la sécurité.

NOTE 2 Dans les processus par lots, un SIS peut être utilisé pour sélectionner différents points de consigne ou différentes fonctions logiques selon la formule qui a été utilisée. Dans ces cas, l'interface opérateur peut être utilisée pour faire le choix requis.

NOTE 3 La fourniture d'informations incorrectes depuis le BPCS vers le SIS ne doit pas compromettre la sécurité.

11.7.2 Exigences relatives à l'interface de maintenance/d'ingénierie

11.7.2.1 La conception de l'interface de maintenance/d'ingénierie du SIS de PE doit garantir qu'aucune défaillance de cette interface ne compromettra l'aptitude du SIS à conduire le processus à un état de sécurité. Ceci peut nécessiter la déconnexion des interfaces de maintenance/d'ingénierie, tels que les dispositifs de programmation, pendant l'exploitation normale du SIS.

11.7.2.2 L'interface de maintenance/d'ingénierie doit fournir la protection de sécurité des accès à chacune des fonctions suivantes:

- mode opérationnel du SIS, programme, données, moyens de désactiver la communication des alarmes, essai, dérivation, maintenance;
- diagnostic du SIS, services de vote majoritaire et de traitement d'anomalie;

11.7.1.2 The design of the SIS shall minimize the need for operator selection of options and the need to bypass the system while the unit is running. If the design does require the use of operator actions, the design should include facilities for protection against operator error.

NOTE If the operator has to select a particular option, there should be a repeat confirmation step.

11.7.1.3 Bypass switches shall be protected by key locks or passwords to prevent unauthorized use.

11.7.1.4 The SIS status information that is critical to maintaining the SIL shall be available as part of the operator interface. This information may include

- where the process is in its sequence;
- indication that SIS protective action has occurred;
- indication that a protective function is bypassed;
- indication that automatic action(s) such as degradation of voting and/or fault handling has occurred;
- status of sensors and final elements;
- the loss of energy where that energy loss impacts safety;
- the results of diagnostics;
- failure of environmental conditioning equipment which is necessary to support the SIS.

11.7.1.5 The SIS operator interface design shall be such as to prevent changes to SIS application software. Where safety information needs to be transmitted from the BPCS to the SIS, then systems should be used which can selectively allow writing from the BPCS to specific SIS variables. Equipment or procedures should be applied to confirm that the proper selection has been transmitted and received by the SIS and does not compromise the safety functionality of the SIS.

NOTE 1 If the options or bypasses are selected in the BPCS and downloaded to the SIS then failures in the BPCS may interfere with the ability of the SIS to operate on demand. If this can occur then the BPCS will become safety related.

NOTE 2 In batch processes an SIS may be used to select different set points or logic functions depending on the recipe being used. In these cases the operator interface may be used to make the required selection.

NOTE 3 Provision of incorrect information from the BPCS to the SIS shall not compromise safety.

11.7.2 Maintenance/engineering interface requirements

11.7.2.1 The design of PE SIS maintenance/engineering interface shall ensure that any failure of this interface shall not adversely affect the ability of the SIS to bring the process to a safe state. This may require disconnecting of maintenance/engineering interfaces, such as programming panels, during normal SIS operation.

11.7.2.2 The maintenance/engineering interface shall provide the following functions with access security protection to each

- SIS operating mode, program, data, means of disabling alarm communication, test, bypass, maintenance;
- SIS diagnostic, voting and fault handling services;

- ajouter, supprimer ou modifier le logiciel d'application;
- données nécessaires pour dépanner le SIS;
- dans le cas où des dérivations sont requises, il convient qu'elles soient installées de telle manière que les alarmes et les dispositifs manuels d'arrêt ne soient pas désactivés.

NOTE Les questions se rapportant au logiciel ne s'appliquent qu'aux SIS utilisant la technologie PE.

11.7.2.3 L'interface de maintenance/d'ingénierie ne doit pas être utilisée comme interface opérateur.

11.7.2.4 L'activation et la désactivation de l'accès à la lecture/écriture ne doivent être faites que par une configuration ou un processus de programmation utilisant l'interface de maintenance/ ingénierie, avec la documentation et les mesures de sécurité appropriées.

11.7.3 Exigences relatives à l'interface de communication

11.7.3.1 La conception de l'interface de communication du SIS doit garantir qu'aucune défaillance de cette interface de communication ne compromettra l'aptitude du SIS à conduire le processus à un état de sécurité.

11.7.3.2 Le SIS doit pouvoir communiquer avec le BPCS et les périphériques sans impact sur la SIF.

11.7.3.3 L'interface de communication doit être suffisamment robuste pour résister aux interférences électromagnétiques, y compris les surtensions, sans entraîner une défaillance dangereuse de la SIF.

11.7.3.4 L'interface de communication doit être apte à assurer la communication entre des dispositifs référencés à différents potentiels électriques de mise à la terre.

NOTE Un autre moyen de communication (par exemple, fibres optiques) peut être nécessaire.

11.8 Exigences relatives à la maintenance ou à la conception des tests

11.8.1 La conception doit tenir compte des essais du SIS, dans sa globalité ou par parties. Dans le cas où l'intervalle entre les temps d'arrêt programmés du processus est plus grand que l'intervalle entre les tests périodiques, des fonctions d'essai en ligne sont requises.

NOTE Le terme «de bout en bout» signifie le déroulement du processus de l'extrémité côté capteur jusqu'à l'extrémité côté actionnement.

11.8.2 Lorsque les tests périodiques en ligne sont prescrits, les dispositifs d'essai doivent faire partie intégrante de la conception du SIS, afin de tester les défaillances non détectées.

11.8.3 Lorsque des dispositifs d'essai et/ou de dérivation sont inclus dans le SIS, ils doivent être conformes aux points suivants:

- le SIS doit être conçu selon les exigences de test et de maintenance définies dans les spécifications des exigences concernant la sécurité;
- l'opérateur doit être alerté lors de la dérivation d'une partie quelconque du SIS, par l'intermédiaire d'une alarme et/ou d'une procédure opérationnelle.

11.8.4 Le forçage des entrées et des sorties d'un SIS de PE ne doit pas être utilisé comme faisant partie:

- d'un logiciel d'application;

- add, delete, or modify application software;
- data necessary to troubleshoot the SIS;
- where bypasses are required they should be installed such that alarms and manual shutdown facilities are not disabled.

NOTE Software issues apply only to SIS using PE technology.

11.7.2.3 The maintenance/engineering interface shall not be used as the operator interface.

11.7.2.4 Enabling and disabling the read-write access shall be carried out only by a configuration or programming process using the maintenance/engineering interface with appropriate documentation and security measures.

11.7.3 Communication interface requirements

11.7.3.1 The design of the SIS communication interface shall ensure that any failure of the communication interface shall not adversely affect the ability of the SIS to bring the process to a safe state.

11.7.3.2 The SIS shall be able to communicate with the BPCS and peripherals with no impact on the SIF.

11.7.3.3 The communication interface shall be sufficiently robust to withstand electro-magnetic interference including power surges without causing a dangerous failure of the SIF.

11.7.3.4 The communication interface shall be suitable for communication between devices referenced to different electrical ground potentials.

NOTE An alternate medium (for example, fibre optics) may be required.

11.8 Maintenance or testing design requirements

11.8.1 The design shall allow for testing of the SIS either end-to-end or in parts. Where the interval between scheduled process downtime is greater than the proof test interval, then on-line testing facilities are required.

NOTE The term end-to-end means from process fluid at sensor end to process fluid at actuation end.

11.8.2 When on-line proof testing is required, test facilities shall be an integral part of the SIS design to test for undetected failures.

11.8.3 When test and/or bypass facilities are included in the SIS, they shall conform with the following.

- The SIS shall be designed in accordance with the maintenance and testing requirements defined in the safety requirement specifications.
- The operator shall be alerted to the bypass of any portion of the SIS via an alarm and/or operating procedure.

11.8.4 Forcing of inputs and outputs in PE SIS shall not be used as a part of

- application software;

- d'une (de) procédure(s) opérationnelle(s);
- de la maintenance, sauf indication contraire ci-dessous.

Le forçage des entrées et des sorties ne doit pas être permis sans mettre le SIS hors service, sauf s'il est complété par des procédures et une sécurité d'accès. Ce forçage doit faire l'objet d'une annonce ou d'une alarme, suivant les cas.

11.9 Probabilité de défaillance de la SIF

11.9.1 La probabilité de défaillance sur sollicitation de chaque fonction instrumentée de sécurité doit être égale ou inférieure à l'objectif de niveau de défaillance, comme cela est spécifié par les spécifications des exigences relatives à la sécurité. Ceci doit être vérifié par calcul.

NOTE 1 Dans le cas de fonctions instrumentées de sécurité fonctionnant dans le mode sollicitation, il convient que la mesure de défaillance cible soit exprimée en termes de probabilité moyenne de défaillance, afin que les fonctions pour lesquelles le système a été conçu soient exécutées lorsqu'elles sont requises, comme cela est déterminé par le niveau d'intégrité de sécurité de la fonction instrumentée de sécurité (voir le Tableau 3).

NOTE 2 Dans le cas d'une fonction instrumentée de sécurité fonctionnant dans le mode continu, il convient que l'objectif de niveau de défaillance soit exprimé en termes de probabilité d'une défaillance dangereuse par heure, comme cela est déterminé par le niveau d'intégrité de sécurité de la fonction instrumentée de sécurité (voir le Tableau 4).

NOTE 3 Il est nécessaire de quantifier séparément la probabilité de défaillance pour chaque fonction instrumentée de sécurité, car différents modes de défaillance des composants peuvent s'appliquer et l'architecture du SIS (en termes de redondance) peut également changer.

NOTE 4 L'objectif de niveau de défaillance peut être une valeur spécifiée de la probabilité moyenne de défaillance sur sollicitation ou du taux des défaillances dangereuses dérivé d'une analyse quantitative ou de la plage spécifiée associée au SIL, si elle a été déterminée par des méthodes qualitatives.

11.9.2 La probabilité de défaillance calculée de chaque fonction instrumentée de sécurité, due aux défaillances du matériel, doit tenir compte:

a) de l'architecture du SIS, du fait qu'il se rapporte à chaque fonction instrumentée de sécurité considérée;

b) du taux estimé des défaillances de chaque sous-système, dû aux anomalies aléatoires du matériel, dans tous les modes qui peuvent provoquer une défaillance dangereuse du SIS, mais qui sont détectés par les essais de diagnostic;

c) du taux estimé des défaillances de chaque sous-système, dû aux anomalies aléatoires du matériel, dans tous les modes pouvant provoquer une défaillance dangereuse du SIS, mais qui ne sont pas détectés par les essais de diagnostic;

   NOTE Les taux estimés des défaillances d'un sous-système peuvent être déterminés par une analyse des modes de défaillance quantifiée, à la conception, en utilisant les données de défaillance de composants ou de sous-systèmes, à partir d'une source industrielle reconnue ou à partir de l'expérience d'une utilisation antérieure du sous-système dans le même environnement que pour l'application prévue; dans ce cas le temps d'exploitation antérieur devrait être suffisant pour démontrer les taux de défaillance annoncés, sur une base statistique, avec une limite inférieure de confiance, mono-latérale, d'au moins 70 %.

d) de la susceptibilité du SIS aux défaillances de cause commune;

e) de la couverture de diagnostic de tous les essais périodiques de diagnostic (déterminée en accord avec la CEI 61511-2), de l'intervalle des essais de diagnostic associé et de la fiabilité des dispositifs de diagnostic;

f) des intervalles auxquels les tests périodiques sont entrepris;

g) des temps de réparation relatifs aux défaillances détectées;

h) du taux estimé des défaillances dangereuses de tout processus de communication, en tous modes, qui peuvent provoquer une défaillance dangereuse du SIS (détectées et non détectées par les essais de diagnostic);

i) du taux estimé des défaillances dangereuses de toute réponse humaine, en tous modes, qui peuvent provoquer une défaillance dangereuse du SIS (détectées et non détectées par les essais de diagnostic);

- operating procedure(s);
- maintenance, except as noted below.

Forcing of inputs and outputs without taking the SIS out of service shall not be allowed unless supplemented by procedures and access security. Any such forcing shall be announced or set off an alarm, as appropriate.

11.9 SIF probability of failure

11.9.1 The probability of failure on demand of each safety instrumented function shall be equal to, or less than, the target failure measure as specified in the safety requirement specifications. This shall be verified by calculation.

NOTE 1 In the case of safety instrumented functions operating in the demand mode of operation, the target failure measure should be expressed in terms of the average probability of failure to perform its design function on demand, as determined by the safety integrity level of the safety instrumented function (see Table 3).

NOTE 2 In the case of a safety instrumented function operating in the continuous mode of operation, the target failure measure should be expressed in terms of the frequency of a dangerous failure per hour, as determined by the safety integrity level of the safety instrumented function (see Table 4).

NOTE 3 It is necessary to quantify the probability of failure separately for each safety instrumented function because different component failure modes could apply and the architecture of the SIS (in terms of redundancy) may also vary.

NOTE 4 The target failure measure may be a specified value of average probability of failure on demand or dangerous failure rate derived from a quantitative analysis or the specified range associated with the SIL if it has been determined by qualitative methods.

11.9.2 The calculated probability of failure of each safety instrumented function due to hardware failures shall take into account

a) the architecture of the SIS as it relates to each safety instrumented function under consideration;

b) the estimated rate of failure of each subsystem, due to random hardware faults, in any modes which would cause a dangerous failure of the SIS but which are detected by diagnostic tests;

c) the estimated rate of failure of each subsystem, due to random hardware faults, in any modes which would cause a dangerous failure of the SIS which are undetected by the diagnostic tests;

   NOTE The estimated rates of failure of a subsystem can be determined by a quantified failure-mode analysis of the design using component or subsystem failure data from a recognized industry source or from experience of the previous use of the subsystem in the same environment as for the intended application, and in which the experience is sufficient to demonstrate the claimed mean time to failure on a statistical basis to a single-sided lower confidence limit of at least 70 %.

d) the susceptibility of the SIS to common cause failures;

e) the diagnostic coverage of any periodic diagnostic tests (determined according to IEC 61511-2), the associated diagnostic test interval and the reliability for the diagnostic facilities;

f) the intervals at which proof tests are undertaken;

g) the repair times for detected failures;

h) the estimated rate of dangerous failure of any communication process in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);

i) the estimated rate of dangerous failure of any human response in any modes which would cause a dangerous failure of the SIS (both detected and undetected by diagnostic tests);

j) de la susceptibilité aux perturbations électromagnétiques (CEM) (par exemple, selon la CEI 61326-1);

k) de la susceptibilité aux conditions climatiques et mécaniques (par exemple, selon la CEI 60654-1 et la CEI 60654-3).

NOTE 1 Des méthodes de modélisation sont disponibles et il appartient à l'analyste de déterminer la plus appropriée et cela devrait dépendre des circonstances. Les méthodes disponibles comprennent (voir la CEI 61508-6, Annexe B:

– la simulation;

– l'analyse cause-conséquence;

– l'analyse par arbre de panne;

– les modèles de Markov;

– les diagrammes de fiabilité.

NOTE 2 L'intervalle des essais de diagnostic ainsi que le temps de réparation qui en découle, constituent le temps moyen jusqu'au rétablissement (voir le VEI 191-13-08), qui est pris en compte dans le modèle de fiabilité.

12 Exigences relatives au logiciel d'application, incluant les critères de sélection pour le logiciel utilitaire

Cet article prend en compte:

– trois types de logiciels:

- les logiciels d'application;
- les logiciels utilitaires, c'est-à-dire, les outils logiciels utilisés pour développer et vérifier le logiciel d'application;
- les logiciels intégrés, c'est-à-dire, les logiciels faisant partie de l'électronique programmable (PE).

– trois types de langages de développement du logiciel:

- les langages de programme figé (FPL);
- les langages de variabilité limitée (LVL);
- les langages de variabilité totale (FVL).

Cette norme est limitée aux logiciels d'application développés en utilisant le FPL ou le LVL. Les exigences suivantes conviennent au développement et à la modification des logiciels d'application jusqu'au SIL 3. Par conséquent, cette norme ne fait pas de différence entre les SIL 1, 2 et 3.

Le développement et les modifications d'un logiciel d'application qui utilise le FPL ou le LVL, jusqu'au SIL 3, doivent être conformes à cette norme. Le développement et les modifications d'un logiciel d'application de SIL4 doivent être conformes à la CEI 61508. Le développement et les modifications d'un logiciel d'application qui utilise le FVL doivent être conformes à la CEI 61508.

Le logiciel utilitaire (ainsi que le manuel de sécurité du constructeur, qui définit comment le système de PE peut être appliqué en toute sécurité), doit être choisi et appliqué conformément aux exigences de 12.4.4. Le choix du logiciel intégré doit être conforme à 11.5.

12.1 Exigences relatives au cycle de vie de sécurité du logiciel d'application

12.1.1 Objectifs

12.1.1.1 Les objectifs de ce paragraphe sont:

- de définir les activités nécessaires pour développer le logiciel d'application pour chaque sous-système programmé du SIS;

j) the susceptibility to EMC disturbances (for example, according to IEC 61326-1);

k) the susceptibility to climatic and mechanical conditions (for example, according to IEC 60654-1 and IEC 60654-3).

NOTE 1 Modelling methods are available and the most appropriate method is a matter for the analyst and should depend on the circumstances. Available methods include (see IEC 61508-6, Annex B)

– simulation;

– cause consequence analysis;

– fault-tree analysis;

– Markov models;

– reliability block diagrams.

NOTE 2 The diagnostic test interval and the subsequent time for repair together constitute the mean time for restoration (see IEV 191-13-08) which should be considered in the reliability model.

12 Requirements for application software, including selection criteria for utility software

This clause recognizes

– three types of software:
  - application software;
  - utility software, i.e., the software tools used to develop and verify the application software;
  - embedded software, i.e., the software supplied as part of the PE;
– three types of software development language:
  - fixed program languages (FPL);
  - limited variability languages (LVL);
  - full variability languages (FVL).

This standard is limited to application software developed using FPL or LVL. The following requirements are suitable for the development and modification of application software up to SIL 3. Therefore, this standard does not differentiate between SIL 1, 2 and 3.

The development and modification of application software using FPL or LVL up to SIL 3 shall comply with this standard. The development and modification of SIL4 application software shall comply with IEC 61508. The development and modification of application software using FVL shall comply with IEC 61508.

Utility software (together with the manufacturer safety manual which defines how the PE system can be safely applied) shall be selected and applied in conformance with the requirements of 12.4.4. The selection of embedded software shall comply with 11.5.

12.1 Application software safety life-cycle requirements

12.1.1 Objectives

12.1.1.1 The objectives of this clause are:

- to define the activities required to develop the application software for each programmed SIS subsystem;

- de définir comment choisir, commander et appliquer le logiciel utilitaire utilisé pour développer le logiciel d'application;
- d'assurer qu'une planification adéquate existe pour garantir que les objectifs de la sécurité fonctionnelle affectés au logiciel d'application seront tenus.

NOTE La Figure 10 illustre le domaine d'application de l'Article 12 dans le cycle de vie de sécurité de l'application.

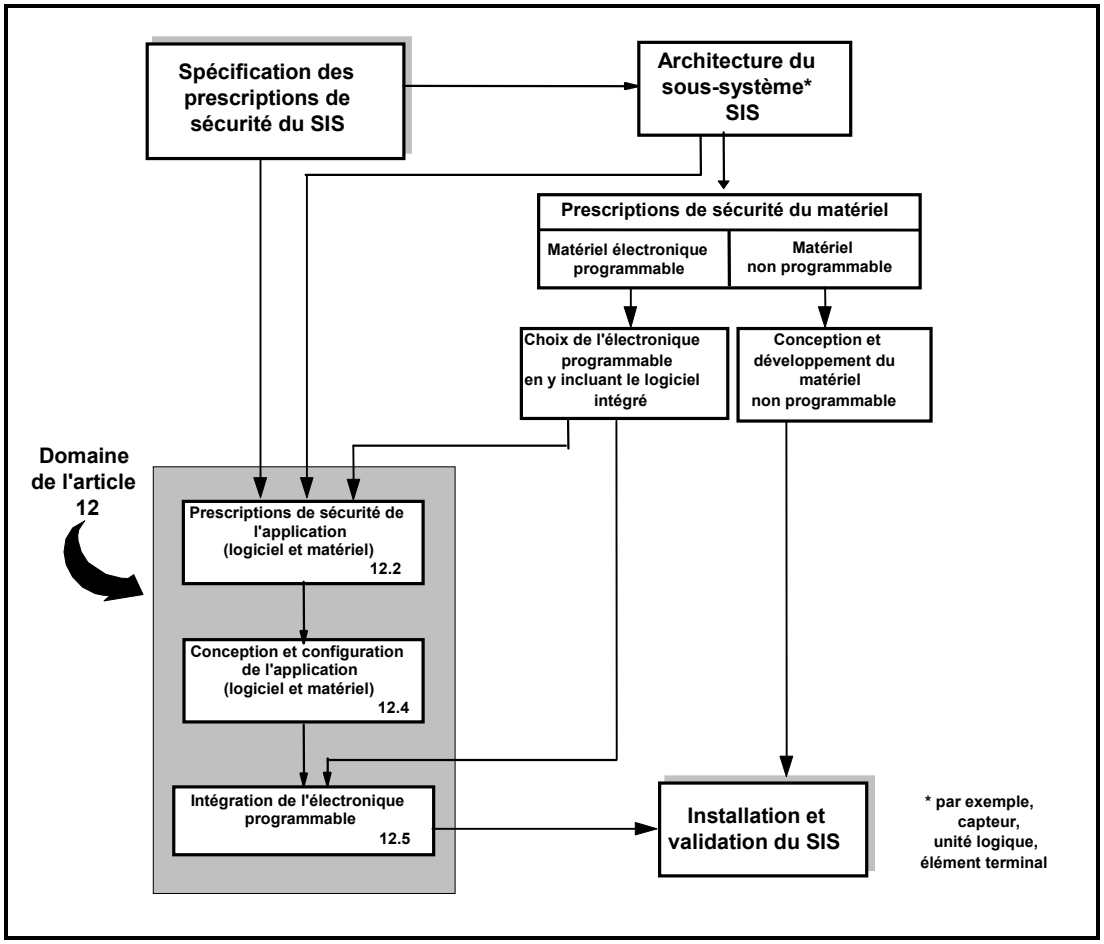


Figure 10 – Cycle de vie de sécurité du logiciel d'application et ses relations avec le cycle de vie de sécurité du SIS

12.1.2 Exigences

12.1.2.1 Un cycle de vie de sécurité relatif au développement du logiciel d'application, qui satisfait aux exigences de cet article, doit être spécifié pendant la planification de la sécurité et doit être intégré au cycle de vie de sécurité du SIS.

12.1.2.2 Chaque phase du cycle de vie de sécurité du logiciel d'application doit être définie en termes de ses activités élémentaires, de ses objectifs, de ses informations d'entrée prescrites et de ses résultats de sortie, des exigences de vérification (voir 12.7) et des responsabilités (voir le Tableau 7 et la Figure 11).

NOTE 1 À condition que le cycle de vie de sécurité du logiciel d'application satisfasse aux exigences du Tableau 7, il est acceptable d'adapter la profondeur, le nombre et la quantité de travail des phases du modèle en V (voir la Figure 12), afin de tenir compte de l'intégrité de sécurité et de la complexité du projet.

NOTE 2 Le type de langage logiciel utilisé (FPL, LVL ou FVL) et l'adéquation du langage aux fonctions de l'application peut avoir une influence sur l'étendue des phases du modèle en V.

- to define how to select, control, and apply the utility software used to develop the application software;
- to ensure that adequate planning exists so that the functional safety objectives allocated to the application software are met.

NOTE Figure 10 illustrates the scope of clause 12 within the application safety life cycle.

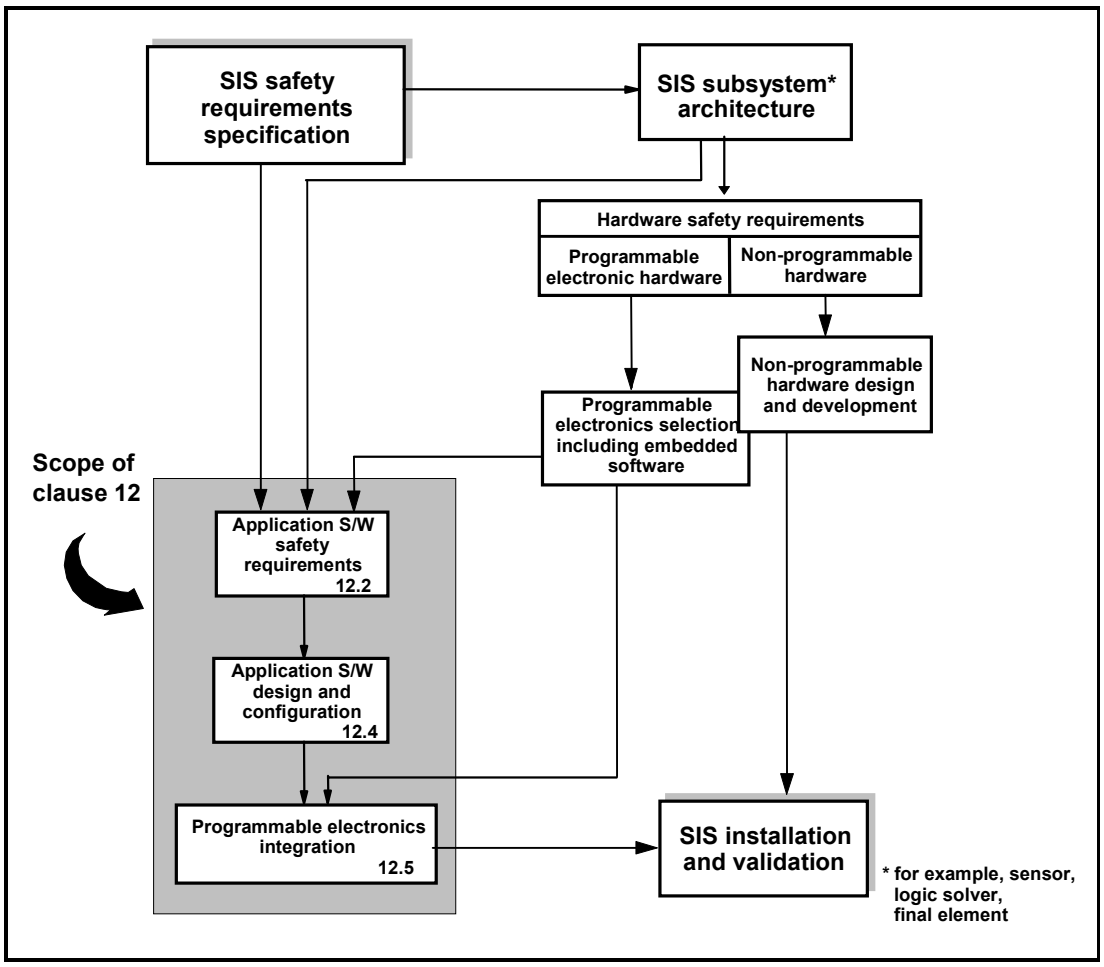


Figure 10 – Application software safety life cycle and its relationship to the SIS safety life cycle

12.1.2 Requirements

12.1.2.1 A safety life cycle for the development of application software which satisfies the requirements of this clause shall be specified during safety planning and integrated with the SIS safety life cycle.

12.1.2.2 Each phase of the application software safety life cycle shall be defined in terms of its elementary activities, objectives, required input information and output results, verification requirements (see 12.7) and responsibilities (see Table 7 and Figure 11).

NOTE 1 Provided that the application software safety life cycle satisfies the requirements of Table 7, it is acceptable to tailor the depth, number and size of the phases of the V-model (see Figure 12) to take account of the safety integrity and the complexity of the project.

NOTE 2 The type of software language used (FPL, LVL or FVL) and the closeness of the language to the application functions may impact the scope of the V-model phases.

NOTE 3 Les spécifications des exigences de sécurité du logiciel d'application peuvent être incluses dans les spécifications des exigences de sécurité du SIS.

NOTE 4 Le plan de validation du logiciel d'application peut être inclus dans le plan de validation global du SIS ou d'un sous-système du SIS.

12.1.2.3 Le dispositif de PE, qui met en oeuvre le logiciel d'application, doit convenir à l'intégrité de sécurité requise par chaque SIF qu'il dessert.

12.1.2.4 Les méthodes, les techniques et les outils doivent être choisis et appliqués pour chaque phase de cycle de vie, de manière à:

- minimiser le risque d'introduire des anomalies dans le logiciel d'application;
- révéler et éliminer les anomalies qui existent déjà dans le logiciel;
- assurer que les anomalies restantes dans le logiciel ne conduiront pas à des résultats inacceptables;
- assurer que le logiciel peut être maintenu durant toute la vie du SIS;
- démontrer que le logiciel a la qualité prescrite.

NOTE Il convient que le choix des méthodes et des techniques dépende de circonstances spécifiques. Les facteurs intervenant dans cette décision sont susceptibles d'inclure:

– la quantité de logiciels;

– le degré de complexité;

– le niveau d'intégrité de sécurité du SIS;

– les conséquences en cas de défaillance;

– le degré de normalisation des éléments de conception.

12.1.2.5 Chaque phase du cycle de vie de sécurité du logiciel d'application doit être vérifiée (voir 12.7) et les résultats doivent être disponibles (voir 19).

12.1.2.6 Si, à un stade quelconque du cycle de vie de sécurité du logiciel, il est nécessaire d'effectuer une modification portant sur une phase précédente du cycle de vie, cette phase antérieure du cycle de vie de sécurité, ainsi que les phases suivantes, doivent alors être ré-examinées et, si des modifications sont requises, répétées et revérifiées.

12.1.2.7 Le logiciel d'application, le matériel du SIS et le logiciel intégré, et le logiciel utilitaire (outils) doivent être soumis à la gestion de configuration (voir 5.2.7).

12.1.2.8 La planification des essais doit être effectuée. Il convient que les points suivants soient abordés:

- les règles d'intégration du logiciel et du matériel;
- les scénarii d'essai et les données d'essai;
- les types d'essais à exécuter;
- l'environnement d'essai comprenant les outils, les logiciels d'aide et la description de la configuration;
- les critères d'essai sur lesquels la fin des essais sera jugée;
- les lieux physiques (par exemple, usine ou site);
- la dépendance à l'égard d'une fonctionnalité externe;
- le personnel approprié;
- les non-conformités.

NOTE 3 The application software safety requirements specifications may be included as part of the SIS safety requirements specifications.

NOTE 4 The application software validation plan may be included as part of the overall SIS or SIS subsystem validation plan.

12.1.2.3 The PE device that implements the application software shall be suitable for the safety integrity required by each SIF it services.

12.1.2.4 Methods, techniques and tools shall be selected and applied for each life-cycle phase so as to

- minimize the risk of introducing faults into the application software;
- reveal and remove faults that already exist in the software;
- ensure that the faults remaining in the software will not lead to unacceptable results;
- ensure that the software can be maintained throughout the lifetime of the SIS;
- demonstrate that the software has the required quality.

NOTE The selection of methods and techniques should depend upon the specific circumstances. The factors in this decision are likely to include

– amount of software;

– degree of complexity;

– safety integrity level of the SIS;

– consequence in the event of failure;

– degree of standardization of design elements.

12.1.2.5 Each phase of the application software safety life cycle shall be verified (see 12.7) and the results shall be available (see Clause 19).

12.1.2.6 If at any stage of the application software safety life cycle, a change is required pertaining to an earlier life-cycle phase, then that earlier safety life-cycle phase and the following phases shall be re-examined and, if changes are required, repeated and re-verified.

12.1.2.7 Application software, the SIS hardware and embedded software and utility software (tools) shall be subject to configuration management (see 5.2.7).

12.1.2.8 Test planning shall be carried out. The following issues should be addressed:

- the policy for integration of software and hardware;
- test cases and test data;
- types of tests to be performed;
- test environment including tools, support software and configuration description;
- test criteria on which the completion of the test will be judged;
- physical location(s) (for example, factory or site);
- dependence on external functionality;
- appropriate personnel;
- nonconformances.

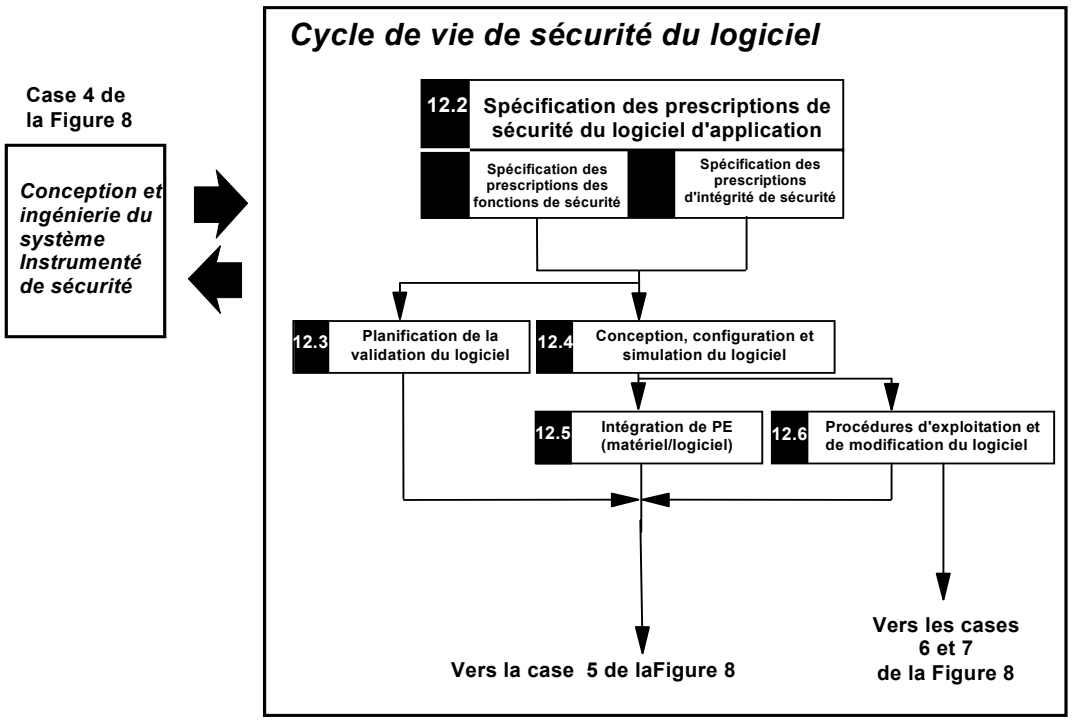


Figure 11 – Cycle de vie de sécurité du logiciel d'application (en phase de réalisation)

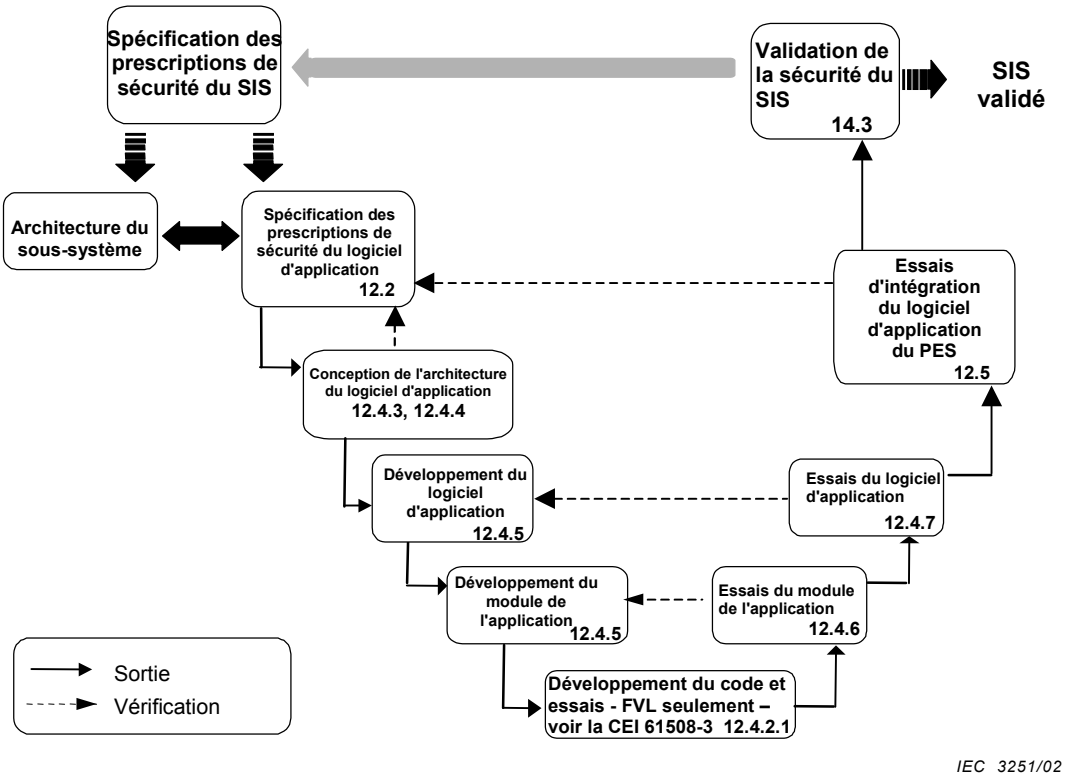


Figure 12 – Cycle de vie de développement du logiciel (modèle en V)

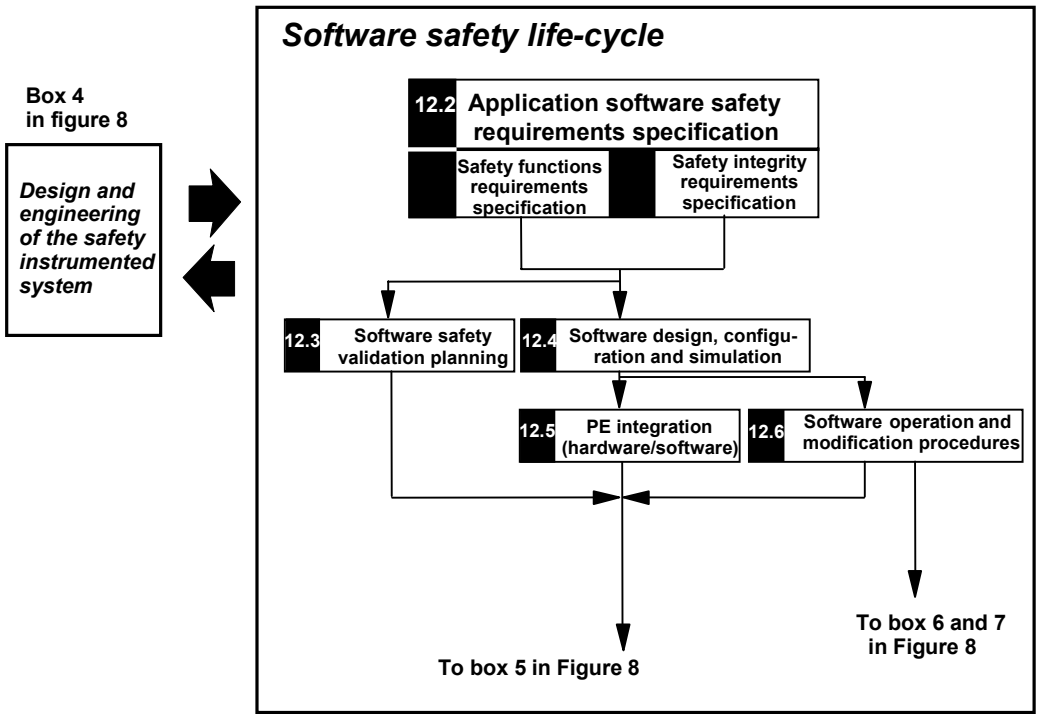


Figure 11 – Application software safety life cycle (in realization phase)

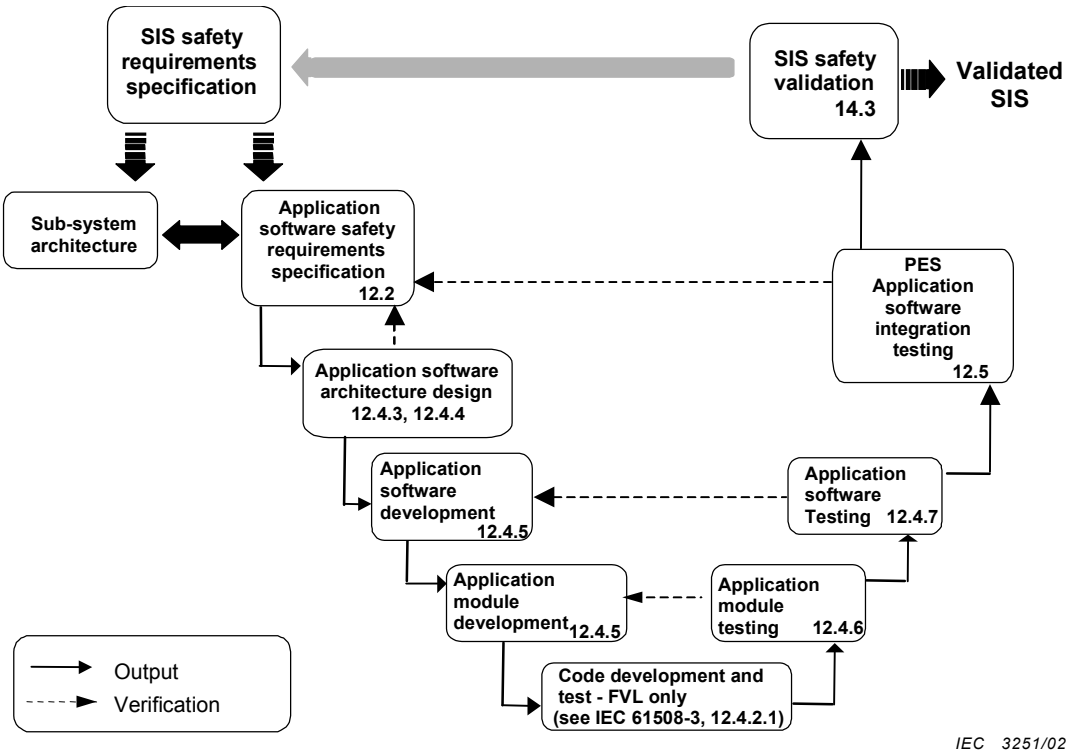


Figure 12 – Software development life cycle (the V-model)

Tableau 7 – Cycle de vie de sécurité du logiciel d'application: vue d'ensemble

Phase du cycle de vie de sécurité		Objectifs	Article des prescrip-tions	Informations requises	Résultats requis
Numéro de case de la Figure 11	Titre				
12.2	Spécification des exigences de sécurité du logiciel d'application	Spécifier les exigences des fonctions instrumentées de sécurité du logiciel pour chaque fonction du SIS nécessaire à la mise en oeuvre des fonctions instrumentées de sécurité requises; Spécifier les exigences d'intégrité de sécurité du logiciel pour chacune des fonctions instrumentées de sécurité affectées au SIS.	12.2.2	Spécification des exigences de sécurité du SIS. Manuels de sécurité du SIS choisi. Architecture du SIS.	Spécification des exigences de sécurité du logiciel d'application du SIS; Informations de vérification.
12.3	Planification de la validation de sécurité du logiciel d'application.	Développer un plan permettant de valider la sécurité du logiciel.	12.3.2	Spécification des exigences de sécurité du logiciel d'application du SIS.	Plan de validation de la sécurité du logiciel d'application du SIS; Informations de vérification.
12.4	Conception et développe-ment du logiciel d'application.	Architecture: Créer une architecture logicielle conforme aux exigences spécifiées pour la sécurité du logiciel. Passer en revue et évaluer les exigences imposées au logiciel par l'architecture matérielle du SIS.	12.4.3	Spécification des exigences de sécurité du logiciel d'application du SIS. Manuels de conception de l'architecture du matériel du SIS.	Description de la conception de l'architecture; par exemple, ségrégation du logiciel d'application en sous-systèmes relatifs au processus et au (aux) SIL; par exemple, reconnaissance de modules logiciels d'application commune, telles que séquences de pompes ou de vannes. Architecture du logiciel d'application et spécification d'essai d'intégration de sous-système; Informations de vérification.
	Conception et développe-ment du logiciel d'application.	Outils d'aide et langages de programmation: Identifier un ensemble adéquat d'outils de configuration, de bibliothèque, de gestion, de simulation et d'essai, pour l'ensemble du cycle de vie de sécurité du logiciel (logiciels utilitaires); Spécifier les procédures de développement du logiciel d'application.	12.4.4	Spécification des exigences de sécurité du logiciel d'application du SIS; Description de la conception de l'architecture; Manuels du SIS. Manuel de sécurité de l'unité logique choisie pour le SIS.	Liste des procédures pour l'utilisation des logiciels utilitaires. Informations de vérification.

Table 7 – Application software safety life cycle: overview

Safety life-cycle phase		Objectives	Require-ments clause	Information required	Required results
Figure 11 box number	Title				
12.2	Application software safety requirements specification	To specify the requirements for the software safety instrumented functions for each SIS function necessary to implement the required safety instrumented functions To specify the requirements for software safety integrity for each safety instrumented function allocated to that SIS	12.2.2	SIS safety requirements specification Safety manuals of the selected SIS SIS architecture	SIS application software safety requirements specification Verification information
12.3	Application software safety validation planning	To develop a plan for validating the application software	12.3.2	SIS application software safety requirements specification	SIS application software safety validation plan Verification information
12.4	Application software design and development	Architecture To create a software architecture that fulfils the specified requirements for software safety To review and evaluate the requirements placed on the software by the hardware architecture of the SIS	12.4.3	SIS application software safety requirements specification SIS hardware architecture design manuals	Description of the architecture design, for example, segregation of application S/W into related process sub-system and SIL(s), for example, recognition of common application S/W modules such as pump or valve sequences Application software architecture and sub-system integration test specification Verification information
	Application software design, and development	Support tools and programming languages To identify a suitable set of configuration, library, management, and simulation and test tools, over the whole safety life cycle of the software (utility software) To specify the procedures for development of the application software	12.4.4	SIS application software safety requirements specification Description of the architecture design Manuals of the SIS Safety manual of the selected SIS logic solver	List of procedures for use of utility software Verification information

Phase du cycle de vie de sécurité		Objectifs	Article des prescrip-tions	Informations requises	Résultats requis
Numéro de case de la Figure 11	Titre				
12.4	Conception et développe-ment du logiciel d'application.	Développement du logiciel d'application et développement du module de l'application. Mettre en oeuvre le logiciel d'application qui satisfait aux exigences spécifiées pour la sécurité de l'application.	12.4.5	Description de la conception de l'architecture. Liste des manuels et des procédures du PES choisi pour l'utilisation des logiciels utilitaires.	1) Programme du logiciel d'application (par exemple, diagrammes en blocs fonctionnels, langage à contact); 2) Simulation du programme d'application et essai d'intégration. 3) Spécification des exigences de sécurité de l'application spécifique. 4) Informations de vérification.
12.4	Développe-ment du logiciel d'application utilisant des langages de variabilité totale.	Développement et essai de programmes – FVL seulement: Mettre en œuvre le langage de variabilité totale qui satisfait aux exigences spécifiées pour la sécurité du logiciel.	12.4.6 et 12.4.7	Exigences de spécification de sécurité du logiciel d'application spécifique.	Se référer à la CEI 61508-3.
12.4	Conception et développe-ment du logiciel d'application.	Essais du logiciel et de l'application: 1) Vérifier que les exigences de sécurité du logiciel ont été tenues. 2) Montrer que tous les programmes d'application les sous-systèmes et le système interagissent correctement pour exécuter leurs fonctions attendues et n'exécutent aucune fonction imprévue. Peut être cumulé avec la phase suivante (12.5), soumis à une couverture d'essai satisfaisant.	12.4.6, 12.4.7, 12.7	Spécification d'essais d'intégration et de simulation du programme d'application (essais structurels). Spécification d'essais d'intégration de l'architecture logicielle.	1) Résultats d'essai du logiciel. 2) Système logiciel vérifié et essayé. 3) Informations de vérification.
12.5	Intégration de l'électronique program-mable (matériel et logiciel)	Intégrer le logiciel dans le matériel de l'électronique programmable cible.	12.5.2	Spécification d'essais d'intégration du logiciel et du matériel.	Résultats des essais d'intégration du logiciel et du matériel. Logiciel et matériel vérifiés.
12.3	Validation de la sécurité du SIS.	Valider le fait que le SIS, incluant le logiciel d'application de sécurité, remplit les exigences de sécurité.	12.3	Plans de validation de la sécurité du logiciel et du SIS.	Résultats de validation de la sécurité du logiciel et du SIS.

Safety life-cycle phase		Objectives	Require-ments clause	Information required	Required results
Figure 11 box number	Title				
12.4	Application software design, and development	Application software development and application module development To implement the application software that fulfils the specified requirements for application safety	12.4.5	Description of the architecture design List of manuals and procedures of the selected PES for use of utility software	1) Application software program (for example, function block diagrams, ladder logic) 2) Application program simulation and integration test 3) Special purpose application software safety requirements specification 4) Verification information
12.4	Application program development using full variability languages	Program development and test – FVL only To implement full variability language that fulfils the specified requirements for software safety	12.4.6 and 12.4.7	Special purpose application software safety requirements specification	Refer to IEC 61508-3
12.4	Application software design and development	Application software testing 1) To verify that the requirements for software safety have been achieved 2) To show that all appli-cation program subsystems and systems interact correctly to perform their intended functions and do not perform unintended functions Can be merged with the next phase (12.5) subject to satisfactory test coverage	12.4.6, 12.4.7, 12.7	Application program simulation and integration test specification (structure based testing) Software architecture integration test specification	1) Software test results 2) Verified and tested software system 3) Verification information
12.5	Program-mable elec-tronics integration (hardware and soft-ware)	To integrate the software onto the target programmable electronic hardware	12.5.2	Software and hardware integration test specification	Software and hardware integration test results Verified software and hardware
12.3	SIS safety validation	Validate that the SIS, including the safety application software, meets the safety requirements	12.3	Software and SIS safety validation plans	Software and SIS validation results

12.2 Spécification des exigences de sécurité du logiciel d'application

NOTE Cette phase est la case 12.2 de la Figure 11.

12.2.1 Objectif

12.2.1.1 L'objectif de ce paragraphe est de fournir des exigences relatives à la spécification des exigences de sécurité du logiciel d'application, pour chaque sous-système programmable du SIS nécessaire pour mettre en oeuvre la (les) fonction(s) instrumentée(s) de sécurité requises, cohérentes avec l'architecture du SIS.

NOTE Voir la Figure 13 concernant les relations architecturales entre le matériel et le logiciel.

<table>
<tr><th colspan="3">Architecture du sous-système SIS programmable</th></tr>
<tr><th>Architecture matérielle</th><th colspan="2">Architecture logicielle (l'architecture logicielle consiste en logiciels intégrés et d'applications)</th></tr>
<tr><td rowspan="2">Caractéristiques génériques et spécifiques à l'application concernant le matériel
Exemples :
– Essais de diagnostic
– Processeurs redondants
– Cartes E/S doublées</td><td>Logiciel intégré</td><td>Logiciel d'application</td></tr>
<tr><td>Exemples :
– Pilotes de communications
– Gestionnaire d'anomalies
– Exécutifs</td><td>Exemples :
– Fonctions E/S
– Fonctions dérivées (par exemple vérification des capteurs, si non fournie en tant que service du logiciel intégré)</td></tr>
</table>

IEC 3252/02

Figure 13 – Relations entre les architectures du matériel et du logiciel du SIS

12.2.2 Exigences

12.2.2.1 Une spécification des exigences de sécurité du logiciel d'application doit être développée.

NOTE 1 Un SIS se compose habituellement de trois sous-systèmes architecturaux: capteurs, unité logique et éléments terminaux. En outre les sous-systèmes peuvent avoir des dispositifs redondants pour atteindre le niveau d'intégrité requis.

NOTE 2 Une architecture matérielle de SIS avec des capteurs redondants peut imposer des exigences supplémentaires pour l'unité logique du SIS (par exemple, mise en œuvre d'une logique 1oo2).

NOTE 3 Les exigences de sécurité du logiciel du sous-système du SIS qui ont déjà été spécifiées dans les exigences relatives au SIS (voir l'Article 10), n'ont pas besoin d'être répétées.

NOTE 4 La spécification des exigences de sécurité du logiciel est nécessaire pour identifier les possibilités minimales de la fonctionnalité logicielle de PE et également pour s'opposer au choix de toute fonctionnalité qui aurait comme conséquence un état de non-sécurité.

12.2.2.2 Les informations d'entrée de la spécification des exigences de sécurité du logiciel pour chaque sous-système du SIS doivent inclure:

a) les exigences de sécurité spécifiées de la SIF;

b) les exigences résultant de l'architecture du SIS, et

c) toutes les exigences de la planification de la sécurité (voir l'Article 5).

NOTE 1 Il convient que ces informations soient mises à la disposition du développeur du logiciel d'application.

NOTE 2 Cette prescription ne signifie pas qu'il ne devrait pas y avoir d'itération entre le développeur de l'architecture du SIS, l'organisation responsable de la configuration des dispositifs et le développeur du logiciel d'application. Au fur et à mesure que les exigences de sécurité du logiciel d'application et que la future architecture du logiciel d'application (voir 12.4.3) deviennent plus précises, il peut y avoir un impact sur l'architecture du matériel du SIS et, pour cette raison, une collaboration étroite entre le développeur de l'architecture du SIS, le fournisseur des sous-systèmes du SIS et le développeur du logiciel d'application est essentielle (voir la Figure 5).

12.2 Application software safety requirements specification

NOTE This phase is box 12.2 of Figure 11.

12.2.1 Objective

12.2.1.1 The objective of this clause is to provide requirements for the specification of the application software safety requirements for each programmable SIS subsystem necessary to implement the required safety instrumented function(s) consistent with the architecture of the SIS.

NOTE See Figure 13 for hardware and software architectural relationship.

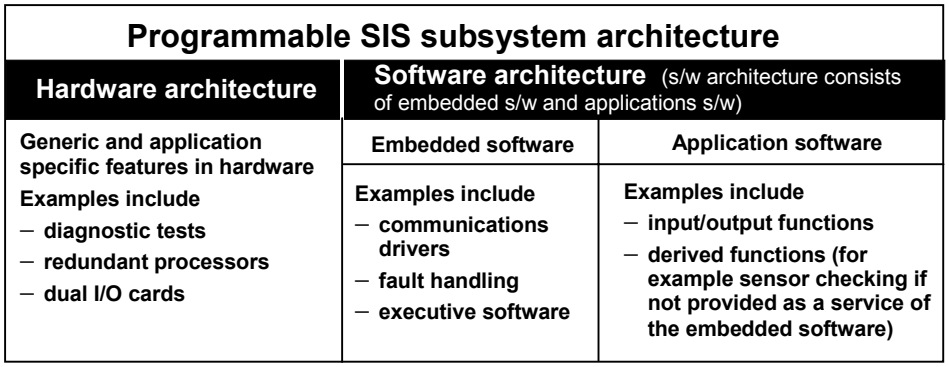


Figure 13 – Relationship between the hardware and software architectures of SIS

12.2.2 Requirements

12.2.2.1 An application software safety requirements specification shall be developed.

NOTE 1 An SIS usually consists of three architectural subsystems: sensors, logic solver and final elements. Furthermore, subsystems could have redundant devices to achieve the required integrity level.

NOTE 2 An SIS hardware architecture with redundant sensors may place additional requirements on the SIS logic solver (for example, implementation of 1oo2 logic).

NOTE 3 The SIS subsystem software safety requirements that have already been specified in the requirements for the SIS (see Clause 10) need not be repeated.

NOTE 4 A software safety requirements specification is required to identify the minimum capabilities of the PE software functionality and also to constrain the selection of any functionality which would result in an unsafe condition.

12.2.2.2 The input to the specification of the software safety requirements for each SIS subsystem shall include

a) the specified safety requirements of the SIF;

b) the requirements resulting from the SIS architecture; and

c) any requirements of safety planning (see Clause 5).

NOTE 1 This information should be made available to the application software developer.

NOTE 2 This requirement does not mean that there should be no iteration between the developer of the SIS architecture, the organization responsible for configuration of the devices and the developer of the application software. As the application software safety requirements and the possible application software architecture (see 12.4.3) become more precise, there may be an impact on the SIS hardware architecture and, for this reason, close cooperation between the SIS architecture developer, the SIS subsystem supplier and the application software developer is essential (see Figure 5).

12.2.2.3 La spécification des exigences relatives à la sécurité du logiciel d'application doit être suffisamment détaillée pour permettre, à la conception et à la mise en œuvre, d'obtenir l'intégrité de sécurité requise et pour permettre d'effectuer une évaluation de la sécurité fonctionnelle. Les points suivants doivent être considérés:

- les fonctions supportées par le logiciel d'application;
- les performances de·capacité et de temps de réponse;
- les interfaces matérielles et opérateurs et leur efficacité opérationnelle;
- tous les modes d'exploitation pertinents du processus, comme cela est indiqué par la spécification des exigences de la sécurité de SIS;
- les actions à prendre concernant les variables erronées du processus, telle qu'une valeur de capteur hors gamme, un circuit ouvert détecté, un court-circuit détecté;
- les tests périodiques et les essais de diagnostic des dispositifs externes (par exemple, capteurs et éléments terminaux);
- l'auto-surveillance du logiciel (qui inclut, par exemple, des chiens de garde pilotés par l'application et la validation de la plage des données);
- la surveillance d'autres dispositifs faisant partie du SIS (par exemple, capteurs et éléments terminaux);
- l'activation des tests périodiques des fonctions instrumentées de sécurité, lorsque le processus est opérationnel;
- les références aux documents d'entrée (par exemple, spécification d'une SIF, configuration ou architecture du SIS, exigences d'intégrité de sécurité du matériel du SIS).

12.2.2.4 Le développeur du logiciel d'application doit passer en revue les informations contenues dans la spécification pour assurer que les exigences sont non ambiguës, cohérentes et compréhensibles. Toutes les insuffisances trouvées dans les exigences de sécurité spécifiées doivent être indiquées au développeur du sous-système du SIS.

12.2.2.5 Il convient que les exigences spécifiées relatives à la sécurité du logiciel soient exprimées et structurées de telle manière qu'elles:

- soient claires pour ceux qui auront à utiliser le document, à n'importe quelle étape du cycle de vie de sécurité du SIS; ceci inclut l'utilisation d'une terminologie et de descriptions non ambiguës et comprises par les opérateurs et par le personnel de maintenance de l'installation industrielle, ainsi que par les programmeurs de l'application;
- soient vérifiables, testables et modifiables;
- soient traçables par rapport à la spécification des exigences de sécurité du SIS.

12.2.2.6 La spécification des exigences de sécurité du logiciel d'application doit donner des informations permettant le choix approprié des équipements. Les points suivants doivent être considérés:

- les fonctions qui permettent au processus d'atteindre ou maintenir un état de sécurité;
- les fonctions relatives à la détection, à la signalisation et à la gestion des anomalies de tous les sous-systèmes du SIS;
- les fonctions relatives aux tests périodiques des fonctions instrumentées de sécurité, en ligne;
- les fonctions relatives aux tests périodiques des fonctions instrumentées de sécurité, hors ligne;
- les fonctions qui permettent la modification du SIS sans risque;

12.2.2.3 The specification of the requirements for application software safety shall be sufficiently detailed to allow the design and implementation to achieve the required safety integrity and to allow an assessment of functional safety to be carried out. The following shall be considered:

- the functions supported by the application software;
- capacity and response time performance;
- equipment and operator interfaces and their operability;
- all relevant modes of operation of the process as specified in the SIS safety requirement specification;
- action to be taken on bad process variable such as sensor value out of range, detected open circuit, detected short circuit;
- proof tests and diagnostic tests of external devices (for example, sensors and final elements);
- software self-monitoring (for example, includes application driven watch-dogs and data range validation);
- monitoring of other devices within the SIS (for example, sensors and final elements);
- enabling periodic testing of safety instrumented functions when the process is operational;
- references to the input documents (for example, specification of the SIF, configuration or architecture of the SIS, hardware safety integrity requirements of the SIS).

12.2.2.4 The application software developer shall review the information in the specification to ensure that the requirements are unambiguous, consistent and understandable. Any deficiencies in the specified safety requirements shall be identified to the SIS subsystem developer.

12.2.2.5 The specified requirements for software safety should be expressed and structured in such a way that they

- are clear to those who will utilize the document at any stage of the SIS safety life cycle; this includes the use of terminology and descriptions which are unambiguous and understood by plant operators and maintainers as well as the application programmers;
- are verifiable, testable, modifiable;
- are traceable back to the specification of the safety requirements of the SIS.

12.2.2.6 The application software safety requirements specification shall provide information allowing proper equipment selection. The following shall be considered:

- functions that enable the process to achieve or maintain a safe state;
- functions related to the detection, annunciation and management of faults in subsystems of the SIS;
- functions related to the periodic testing of safety instrumented functions on-line;
- functions related to the periodic testing of safety instrumented functions off-line;
- functions that allow the SIS to be safely modified;

- les interfaces avec les fonctions non relatives à la sécurité;
- les performances de·capacité et de temps de réponse;
- les niveaux d'intégrité de sécurité pour chacune des fonctions ci-dessus.

NOTE 1 En fonction des propriétés du sous-système du SIS choisi, certaines de ces fonctions peuvent faire partie du logiciel système.

NOTE 2 Les interfaces comprennent les dispositifs de programmation en ligne et hors ligne.

12.3 Planification de la validation de la sécurité du logiciel d'application

NOTE Cette phase est la case 12.3 de la Figure 11.

12.3.1 Objectif

12.3.1.1 L'objectif des exigences de ce paragraphe est d'assurer qu'une planification convenable de la validation du logiciel d'application est réalisée.

12.3.2 Exigences

12.3.2.1 La planification de la validation du logiciel d'application doit être effectuée en accord avec l'Article 15.

12.4 Conception et développement du logiciel d'application

NOTE Cette phase est la case 12.4 de la Figure 11.

12.4.1 Objectifs

12.4.1.1 Le premier objectif des exigences de ce paragraphe est de créer une architecture du logiciel d'application qui est cohérente avec l'architecture du matériel et qui satisfait aux exigences spécifiées pour la sécurité du logiciel (voir 12.2).

12.4.1.2 Le deuxième objectif des exigences de ce paragraphe est de passer en revue et d'évaluer les exigences imposées au logiciel par l'architecture matérielle et par le logiciel intégré au SIS. Ceci inclut les effets secondaires du comportement du matériel/du logiciel du SIS, de la configuration spécifique de l'application du matériel du SIS, de la tolérance aux anomalies inhérentes au SIS et de l'interaction de l'architecture du matériel du SIS et du logiciel intégré avec le logiciel d'application vis-à-vis de la sécurité.

12.4.1.3 Le troisième objectif des exigences du présent paragraphe est de sélectionner un ensemble adéquat d'outils (y compris les logiciels utilitaires), pour développer le logiciel d'application.

12.4.1.4 Le quatrième objectif des exigences de ce paragraphe est de concevoir et de mettre en oeuvre ou de choisir le logiciel d'application qui répond aux exigences spécifiées pour la sécurité du logiciel (voir 12.2), qui est analysable, vérifiable et apte à être modifié sans risque.

12.4.1.5 Le cinquième objectif des exigences de ce paragraphe est de vérifier que les exigences pour la sécurité du logiciel (en termes de fonctions instrumentées de sécurité du logiciel requises) ont été remplies.

12.4.2 Exigences générales

12.4.2.1 Le développement, les essais, la vérification et la validation du programme d'application utilisant le langage de variabilité totale, doivent être conformes à la CEI 61508-3.

- interfaces to non-safety related functions;
- capacity and response time performance;
- the safety integrity levels for each of the above functions.

NOTE 1 Dependent on the properties of the selected SIS subsystem some of these functions may be part of the system software.

NOTE 2 Interfaces include both off-line and on-line modification facilities.

12.3 Application software safety validation planning

NOTE This phase is box 12.3 of Figure 11.

12.3.1 Objective

12.3.1.1 The objective of the requirements of this clause is to ensure that suitable application software validation planning is carried out.

12.3.2 Requirements

12.3.2.1 Application software validation planning shall be carried out in accordance with Clause 15.

12.4 Application software design and development

NOTE This phase is box 12.4 of Figure 11.

12.4.1 Objectives

12.4.1.1 The first objective of the requirements of this clause is to create an application software architecture that is consistent with the hardware architecture and that fulfils the specified requirements for software safety (see 12.2).

12.4.1.2 The second objective of the requirements of this clause is to review and evaluate the requirements placed on the software by the hardware and embedded software architecture of the SIS. These include side-effects of the SIS hardware/software behaviour, the application specific configuration of SIS hardware, the inherent fault tolerance of the SIS and the interaction of the SIS hardware and embedded software architecture with the application software for safety.

12.4.1.3 The third objective of the requirements of this clause is to select a suitable set of tools (including utility software) to develop the application software.

12.4.1.4 The fourth objective of the requirements of this clause is to design and implement or select application software that fulfils the specified requirements for software safety (see 12.2) that is analysable, verifiable and capable of being safely modified.

12.4.1.5 The fifth objective of the requirements of this clause is to verify that the requirements for software safety (in terms of the required software safety instrumented functions) have been achieved.

12.4.2 General requirements

12.4.2.1 The development, test, verification and validation of the full variability language application program shall be in accordance with IEC 61508-3.

12.4.2.2 La méthode de conception doit être cohérente avec les outils de développement et avec les restrictions données pour le sous-système du SIS appliqué.

NOTE Il convient que les restrictions à l'application du sous-système du SIS, nécessaires pour assurer la conformité à la CEI 61511, soient définies dans le manuel de sécurité de l'équipement.

12.4.2.3 Il convient que la méthode de conception et le langage d'application choisis (LVL ou FPL) possèdent des caractéristiques qui facilitent:

a) l'abstraction, la modularité et d'autres caractéristiques qui permettent la maîtrise de la complexité; dans la mesure du possible, il convient que le logiciel soit basé sur des modules logiciels dûment éprouvés, qui peuvent inclure des fonctions de bibliothèque utilisateur et des règles bien définies liant les modules du logiciel;

b) l'expression de:

   — la fonctionnalité, idéalement en tant que description logique ou fonctions algorithmiques;

   — le flux d'informations entre les éléments modulaires des fonctions de l'application;

   — les exigences de séquencement;

   — l'assurance que les fonctions instrumentées de sécurité fonctionnent toujours suivant les contraintes de temps définies;

   — l'absence de comportement indéterminé;

   — l'assurance que les données élémentaires internes ne sont pas dupliquées par erreur, tous les types de données utilisées sont définies et l'action appropriée se produit lorsque les données sont hors gamme ou erronées;

   — les hypothèses de conception et leurs liens.

c) la compréhension par les développeurs et les autres personnes qui en ont besoin, de la conception, à la fois du point de vue de la fonctionalité de l'application et de la connaissance des contraintes de la technologie;

d) la vérification et la validation, y compris la couverture du code du logiciel d'application, la couverture fonctionnelle de l'application intégrée, l'interface avec le SIS et sa configuration de matériel spécifique de l'application;

e) les dispositions qui facilitent la modification du logiciel d'application. Ces dispositions incluent la modularité, la traçabilité et la documentation.

12.4.2.4 La conception réalisée doit:

a) inclure des contrôles d'intégrité des données et des contrôles de vraisemblance;

   NOTE par exemple, contrôles de bout en bout des liaisons, contrôles de limitation de zones adressables des entrées de capteur, contrôles de limitation de zones adressables des paramètres de données et exécution diverse des fonctions de l'application.

b) être traçable par rapport aux exigences;

c) être testable;

d) avoir la capacité d'accepter des modifications, sans risque;

e) maintenir à des minima la complexité et la taille du logiciel d'application du SIF.

12.4.2.5 Lorsque le logiciel d'application doit mettre en œuvre des fonctions instrumentées de sécurité correspondant à différents niveaux d'intégrité de sécurité ou des fonctions non sécuritaires, le logiciel dans son ensemble doit être considéré comme appartenant au niveau d'intégrité de sécurité le plus élevé, à moins qu'une indépendance entre les fonctions instrumentées de sécurité correspondant aux différents niveaux d'intégrité de sécurité puisse être démontrée au niveau de la conception. La justification de l'indépendance des fonctions doit être documentée. Que l'indépendance soit annoncée ou non, le SIL attendu de la fonction de l'application pour chaque SIF doit être identifié.

12.4.2.2 The design method shall be consistent with the development tools and restrictions given for the applied SIS subsystem.

NOTE Restrictions on the application of the SIS subsystem necessary to ensure compliance with IEC 61511 should be defined in the equipment safety manual.

12.4.2.3 The selected design method and application language (LVL or FPL) should possess features that facilitate

a) abstraction, modularity and other features which control complexity; wherever possible, the software should be based on well-proven software modules that may include user library functions and well-defined rules for linking the software modules;

b) expression of

   – functionality, ideally as a logical description or as algorithmic functions;

   – information flow between modular elements of the application functions;

   – sequencing requirements;

   – assurance that safety instrumented functions always operate within the defined time constraints;

   – freedom from indeterminate behaviour;

   – assurance that internal data items are not erroneously duplicated, all used data types are defined and appropriate action occurs when data is out of range or bad;

   – design assumptions and their dependencies.

c) comprehension by developers and others who need to understand the design, both from an application functional understanding and from a knowledge of the constraints of the technology;

d) verification and validation, including coverage of the application software code, functional coverage of the integrated application, the interface with the SIS and its application specific hardware configuration;

e) application software modification. Such features include modularity, traceability and documentation.

12.4.2.4 The design achieved shall

a) include data integrity checks and reasonableness checks;

   NOTE For example, end-to-end checks in communications links, bounds checking on sensor inputs, bounds checking on data parameters and diverse execution of application functions.

b) be traceable to requirements;

c) be testable;

d) have the capacity for safe modification;

e) keep the complexity and size of SIF application software to a minimum.

12.4.2.5 Where the application software is to implement safety instrumented functions of different safety integrity levels or non-safety functions, then all of the software shall be treated as belonging to the highest safety integrity level, unless independence between the safety instrumented functions of the different safety integrity levels can be shown in the design. The justification for independence shall be documented. Whether independence is claimed or not, the intended SIL of each SIF shall be identified.

NOTE 1 La CEI 61511-2 donne des conseils sur la façon de concevoir et de développer le logiciel d'application lorsque les fonctions instrumentées de sécurité et non sécuritaires doivent être mises en oeuvre dans le SIS.

NOTE 2 La CEI 61511-2 donne des conseils sur la façon de concevoir et de développer le logiciel d'application lorsque les SIF de différents SIL doivent être mises en oeuvre dans le SIS.

12.4.2.6 Si des fonctions de bibliothèque du logiciel d'application précédemment développées doivent d'être utilisées en tant qu'éléments de la conception, leur aptitude à satisfaire à la spécification des exigences de sécurité du logiciel d'application (voir 12.2) doit être justifiée. L'aptitude doit être fondée sur:

- la conformité à la CEI 61508-3, lors de l'utilisation d'un FVL; ou
- la conformité à la CEI 61511, lors de l'utilisation d'un FPL ou d'un LVL; ou
- la constatation d'un fonctionnement satisfaisant dans une application similaire, pour laquelle il a été démontré qu'elle a une fonctionnalité similaire ou qu'elle a été soumise aux mêmes procédures de vérification et de validation que celles qui auraient été prévues pour tout logiciel nouvellement développé (voir 11.5.4 et 11.5.5).

NOTE La justification peut être réalisée pendant la planification de sécurité (voir l'Article 6).

12.4.2.7 Au minimum, les informations suivantes doivent être contenues dans la documentation du programme d'application ou dans la documentation associée:

a) l'entité légale (par exemple société, auteur(s));

b) la description;

c) la traçabilité par rapport aux exigences fonctionnelles de l'application;

d) les conventions logiques utilisées;

e) les fonctions standards de bibliothèque utilisées;

f) les entrées et les sorties; et

g) la gestion de configuration incluant un historique des modifications.

12.4.3 Exigences relatives à l'architecture du logiciel d'application

12.4.3.1 La conception de l'architecture du logiciel d'application doit être basée sur la spécification de sécurité du SIS requise, en tenant compte des contraintes de l'architecture au niveau système du SIS. Elle doit être conforme aux exigences relatives à la conception du sous-système sélectionné, à son ensemble d'outils et à son manuel de sécurité.

NOTE 1 L'architecture du logiciel définit les composants et les sous-systèmes principaux du système et du logiciel d'application, comment ils sont interconnectés, et comment les attributs requis, en particulier l'intégrité de sécurité, sont obtenus. Des exemples de modules logiciels système sont les systèmes d'exploitation, les bases de données, les sous-systèmes de communication. Des exemples des modules logiciels d'application sont les fonctions d'application qui sont répliquées dans toute l'installation industrielle.

NOTE 2 Il convient que l'architecture du logiciel d'application soit également déterminée par l'architecture sous-jacente du sous-système du SIS donnée par le fournisseur.

12.4.3.2 La description de la conception de l'architecture du logiciel d'application doit:

a) fournir une description complète de la structure interne et du fonctionnement du sous-système du SIS et de ses composants;

b) inclure les spécifications de tous les composants identifiés, et la description des liaisons et des interactions entre les composants identifiés (logiciel et matériel);

c) identifier les modules logiciels inclus dans le sous-système du SIS, mais non utilisés dans les SIF;

d) décrire l'ordre du traitement logique des données par rapport aux sous-systèmes d'entrée/sortie et la fonctionnalité de l'unité logique, y compris toutes les limitations imposées par des temps de balayage;

NOTE 1 IEC 61511-2 provides guidance on how to design and develop the application software when both safety and non-safety instrumented functions are to be implemented in the SIS.

NOTE 2 IEC 61511-2 provides guidance on how to design and develop the application software when SIF of different SIL are to be implemented in the SIS.

12.4.2.6 If previously developed application software library functions are to be used as part of the design, their suitability in satisfying the specification of requirements for application software safety (see 12.2) shall be justified. Suitability shall be based upon

- compliance to IEC 61508-3 when using FVL; or
- compliance to IEC 61511 when using FPL or LVL; or
- evidence of satisfactory operation in a similar application which has been demonstrated to have similar functionality or having been subject to the same verification and validation procedures as would be expected for any newly developed software (see 11.5.4 and 11.5.5).

NOTE The justification may be developed during safety planning (see Clause 6).

12.4.2.7 As a minimum, the following information shall be contained in the application program documentation or related documentation:

a) legal entity (for example company, author(s));

b) description;

c) traceability to application functional requirements;

d) logic conventions used;

e) standard library functions used;

f) inputs and outputs; and

g) configuration management including a history of changes.

12.4.3 Requirements for application software architecture

12.4.3.1 The design of the application software architecture shall be based on the required SIS safety specification within the constraints of the system architecture of the SIS. It shall comply with the requirements of the selected subsystem design, its tool set and safety manual.

NOTE 1 The software architecture defines the major components and subsystems of system and application software, how they are interconnected, and how the required attributes, particularly safety integrity, are achieved. Examples of system software modules include operating systems, databases, communication subsystems. Examples of application software modules include application functions which are replicated throughout the plant.

NOTE 2 The application software architecture should also be determined by the underlying architecture of the SIS subsystem provided by the supplier.

12.4.3.2 The description of the application software architecture design shall

a) provide a comprehensive description of the internal structure and of the operation of the SIS subsystem and of its components;

b) include the specification of all identified components, and the description of connections and interactions between identified components (software and hardware);

c) identify the software modules included in the SIS subsystem but not used in any SIF;

d) describe the order of the logical processing of data with respect to the input/output sub-systems and the logic solver functionality, including any limitations imposed by scan times;

e) identifier toutes les fonctions non sécuritaires et assurer qu'elles ne peuvent pas affecter le bon fonctionnement des SIF.

NOTE Il est particulièrement important que la documentation de l'architecture soit à jour et complète, vis-à-vis du sous-système du SIS.

12.4.3.3 Il convient que l'ensemble des méthodes et des techniques utilisées pour développer le logiciel d'application soient identifiées et il convient que la justification de leur choix soit explicitée.

NOTE Il convient que ces méthodes et techniques visent à assurer:

– la possibilité de prévoir le comportement du sous-système du SIS;

– la tolérance aux anomalies (cohérente avec le matériel) et l'évitement des anomalies, y compris la redondance et la diversité.

12.4.3.4 Il convient que les méthodes et les techniques utilisées dans la conception du logiciel d'application soient cohérentes avec toutes les contraintes identifiées du manuel de sécurité du sous-système du SIS.

12.4.3.5 Les dispositions mises en œuvre pour maintenir l'intégrité de sécurité de toutes les données doivent être décrites et justifiées. Ces données peuvent inclure des données d'entrée/sortie de l'installation industrielle, des données de communications, des données d'exploitation, des données de maintenance et des données de base de données internes.

NOTE Il y aura itération entre l'architecture matérielle et l'architecture logicielle (voir la Figure 11) et il est donc nécessaire de discuter avec le développeur du matériel des questions concernant, par exemple, la spécification des essais d'intégration du matériel de l'électronique programmable et du logiciel (voir 12.5).

12.4.4 Exigences relatives aux outils supports, au manuel utilisateur et aux langages d'application

12.4.4.1 Un ensemble approprié d'outils doit être choisi, comprenant un sous-ensemble du langage de programmation de l'application, des outils de gestion de configuration, de simulation, des outils bancs d'essai, et lorsque cela est applicable, des outils de mesure de couverture d'essai automatiques.

12.4.4.2 Il convient de considérer la disponibilité des outils adaptés (pas nécessairement ceux utilisés pendant le développement initial du système) destinés à assurer les services appropriés pendant toute la vie du SIS.

NOTE Il convient que le choix des outils de développement dépende de la nature des activités de développement du logiciel d'application, du logiciel intégré et de l'architecture du logiciel (voir 12.4.3).

12.4.4.3 Il convient qu'un ensemble approprié de procédures relatives à l'utilisation des outils soit identifié, en tenant compte des contraintes du manuel de sécurité, des faiblesses connues susceptibles d'introduire des anomalies dans le logiciel d'application et toutes les limitations relatives à la couverture des précédentes vérification et validation.

12.4.4.4 Le langage d'application choisi doit:

- être mis en application en utilisant un traducteur/compilateur qui a été évalué en vue d'établir son aptitude à l'utilisation prévue;
- être totalement défini de façon non ambiguë, ou limité à des caractéristiques définies de façon non ambiguë;
- correspondre aux caractéristiques de l'application;
- comporter des caractéristiques qui facilitent la détection des erreurs de programmation; et
- supporter des caractéristiques adaptées à la méthode de conception.

e) identify all non-SIF and ensure they cannot affect the proper operation of any SIF.

NOTE It is of particular importance that the architecture documentation is up to date and complete with respect to the SIS subsystem.

12.4.3.3 The set of methods and techniques used to develop the application software should be identified and the rationale for their choice should be justified.

NOTE These methods and techniques should aim at ensuring

– the predictability of the behaviour of the SIS subsystem;

– the fault tolerance (consistent with the hardware) and fault avoidance, including redundancy and diversity.

12.4.3.4 The methods and techniques used in the design of the application software should be consistent with any constraints identified in the SIS subsystem safety manual.

12.4.3.5 The features used for maintaining the safety integrity of all data shall be described and justified. Such data may include plant input-output data, communications data, operation data, maintenance data and internal database data.

NOTE There will be iteration between the hardware and software architecture (see Figure 11) and there is therefore a need to discuss with the hardware developer such issues as the test specification for the integration of the programmable electronics hardware and the software (see 12.5).

12.4.4 Requirements for support tools, user manual and application languages

12.4.4.1 A suitable set of tools, including a sub-set of the application programming language, configuration management, simulation, test harness tools, and, when applicable, automatic test coverage measurement tools, shall be selected.

12.4.4.2 The availability of suitable tools (not necessarily those used during initial system development) to supply the relevant services over the whole lifetime of the SIS should be considered.

NOTE The selection of development tools should depend on the nature of the application software development activities, embedded software and the software architecture (see 12.4.3).

12.4.4.3 A suitable set of procedures for use of the tools should be identified, taking into account safety manual constraints, known weaknesses likely to introduce faults into the application software and any limitations on the coverage of earlier verification and validation.

12.4.4.4 The application language selected shall

- be implemented using a translator/compiler that has been assessed to establish its fitness for purpose;
- be completely and unambiguously defined or restricted to unambiguously defined features;
- match the characteristics of the application;
- contain features that facilitate the detection of programming mistakes; and
- support features that match the design method.

12.4.4.5 Dans le cas où 12.4.4.4 ne peut pas être satisfait, une justification du langage utilisé doit alors être donnée lors de la description de la conception de l'architecture du logiciel (voir 12.4.3). La justification doit détailler l'aptitude du langage à remplir l'objectif prévu et toutes les mesures supplémentaires pour traiter tous les inconvénients identifiés du langage.

12.4.4.6 Il convient que les procédures relatives à l'utilisation du langage d'application spécifient de bonnes pratiques de programmation, proscrivent les fonctions logicielles génériques peu sûres (par exemple, fonctions de langage non défini, conceptions non structurées), identifient des contrôles pour détecter des anomalies dans la configuration et spécifient des règles pour la documentation du programme d'application.

12.4.4.7 Le manuel de sécurité doit contenir les rubriques suivantes, en fonction des besoins:

a) l'utilisation des diagnostics pour exécuter des fonctions sûres;

b) une liste de bibliothèques de sécurité certifiées/vérifiées;

c) les essais obligatoires et la logique d'arrêt du système;

d) l'utilisation des chiens de garde;

e) les exigences relatives aux outils et aux langages de programmation et leurs limitations;

f) les niveaux d'intégrité de sécurité auxquels le dispositif ou le système convient.

12.4.4.8 L'aptitude des outils à remplir leurs fonctions doit être vérifiée.

12.4.5 Exigences relatives au développement du logiciel d'application

12.4.5.1 Les informations suivantes doivent être disponibles préalablement au début de la conception détaillée du logiciel d'application:

a) la spécification des exigences de sécurité du logiciel (voir 12.2);

b) la description de la conception de l'architecture du logiciel d'application (voir 12.4.3) comprenant l'identification de la logique de l'application et de la fonctionnalité de tolérance aux anomalies, une liste des données d'entrée et de sortie, des modules logiciels génériques et des outils supports à utiliser, et les procédures de programmation du logiciel d'application.

12.4.5.2 Il convient que le logiciel d'application soit produit d'une manière structurée, en vue d'obtenir:

- la modularité et la fonctionnalité;
- la testabilité de la fonctionnalité (y compris les dispositifs tolérants aux anomalies) et de la structure interne;
- la capacité d'accepter sans risque des modifications;
- la traçabilité vis-à-vis des fonctions de l'application et des contraintes associées et leur explicitation.

NOTE 1 Dans la mesure du possible, il convient que des modules logiciels éprouvés soient utilisés.

12.4.5.3 La conception de chaque module de l'application doit tenir compte de la robustesse, comprenant:

- les contrôles de vraisemblance de chaque variable d'entrée, incluant toutes les variables globales utilisées pour fournir les données d'entrée;

12.4.4.5 When 12.4.4.4 cannot be satisfied, then a justification for the language used shall be documented during application software architecture design description (see 12.4.3). The justification shall detail the fitness for purpose of the language, and any additional measures which address any identified shortcomings of the language.

12.4.4.6 The procedures for use of the application language should specify good programming practice, proscribe unsafe generic software features (for example, undefined language features, unstructured designs), identify checks to detect faults in the configuration and specify procedures for documentation of the application program.

12.4.4.7 The safety manual shall address the following items as appropriate:

a) use of diagnostics to perform safe functions;

b) list of certified/verified safety libraries;

c) mandatory test and system shutdown logic;

d) use of watchdogs;

e) requirements for, and limitations of, tools and programming languages;

f) safety integrity levels for which the device or system is suitable .

12.4.4.8 The suitability of the tools shall be verified.

12.4.5 Requirements for application software development

12.4.5.1 The following information shall be available prior to the start of detailed application software design:

a) the specification of software safety requirements (see 12.2);

b) the description of the application software architecture design (see 12.4.3) including identification of the application logic and fault tolerant functionality, a list of input and output data, the generic software modules and support tools to be used and the procedures for programming the application software.

12.4.5.2 The application software should be produced in a structured way to achieve

- modularity of functionality;
- testability of functionality (including fault tolerant features) and of internal structure;
- the capacity for safe modification;
- traceability to, and explanation of, application functions and associated constraints.

NOTE Wherever possible proven software modules should be used.

12.4.5.3 The design of each application module shall address robustness including

- plausibility checks of each input variable including any global variables used to provide input data;

- la définition complète des interfaces d'entrée et de sortie;
- les contrôles de configuration du système, comprenant l'existence et l'accessibilité des modules matériels et logiciels attendus.

12.4.5.4 La conception de chaque module du logiciel d'application et les essais structuraux à appliquer à chacun d'eux doit être spécifiée.

12.4.5.5 Il convient que le logiciel d'application:

- soit lisible, compréhensible et testable;
- satisfasse aux principes de conception appropriés;
- satisfasse aux exigences ad hoc, spécifiées pendant la planification de la sécurité (voir 5.2.4).

12.4.5.6 Le logiciel d'application doit être passé en revue pour assurer la conformité à la conception spécifiée, aux principes de conception, et aux exigences de planification de la validation de la sécurité.

NOTE La revue du logiciel d'application inclut des techniques telles que les inspections du logiciel, les lectures croisées, et l'analyse formelle. Il convient qu'elle soit utilisée en même temps que la simulation et les essais, pour donner l'assurance que le logiciel d'application satisfait à ses spécifications associées.

12.4.6 Exigences relatives aux essais des modules logiciels de l'application

NOTE Faire l'essai montrant que le module logiciel de l'application satisfait correctement à sa spécification est une activité de vérification – voir également 12.7. C'est la combinaison de la revue et des essais structuraux, qui donne l'assurance qu'un module logiciel de l'application satisfait à sa spécification associée, c'est-à-dire qu'il est vérifié.

12.4.6.1 La configuration de chaque point d'entrée à travers la logique de traitement jusqu'au point de sortie doit être vérifiée par des techniques de revue, de simulation et d'essais, pour confirmer que les données d'E/S sont mises en correspondance avec la logique d'application correcte.

12.4.6.2 Chaque module logiciel de l'application doit être vérifié par des techniques de revue, de simulation et d'essais, pour déterminer si la fonction prévue est correctement exécutée et si les fonctions non attendues sont non exécutées.

Les essais doivent être adaptés au module spécifique à essayer et les points suivants doivent être considérés:

- exploration de toutes les parties du modèle de l'application;
- exploration des frontières des données;
- effets des relations temporelles dus à la séquence d'exécution;
- mise en œuvre de séquence appropriée.

12.4.6.3 Les résultats des essais des modules logiciels de l'application doivent être disponibles.

12.4.7 Exigences relatives aux essais d'intégration du logiciel d'application

NOTE Faire l'essai montrant que le logiciel est correctement intégré est une activité de vérification – voir également 12.7.

12.4.7.1 Les essais du logiciel d'application doivent montrer que tous les modules logiciels de l'application et les composants/sous-systèmes interagissent correctement les uns avec les autres et avec le logiciel intégré de base, de façon à réaliser leur fonction prévue.

- full definition of input and output interfaces;
- system configuration checks including the existence and accessibility of expected hardware and software modules.

12.4.5.4 The design of each application software module and the structural tests to be applied to each application software module shall be specified.

12.4.5.5 The application software should

- be readable, understandable and testable;
- satisfy the relevant design principles;
- satisfy the relevant requirements specified during safety planning (see 5.2.4).

12.4.5.6 The application software shall be reviewed to ensure conformance to the specified design, the design principles, and the requirements of safety validation planning.

NOTE Application software review includes such techniques as software inspections, walk-throughs, and formal analysis. It should be used in conjunction with simulation and testing to provide assurance that the application software satisfies its associated specification.

12.4.6 Requirements for application software module testing

NOTE Testing that the application software module correctly satisfies its specification is a verification activity (see also 12.7). It is the combination of review and structural testing that provides assurance that an application software module satisfies its associated specification, i.e., it is verified.

12.4.6.1 The configuration of each input point through the processing logic to the output point shall be checked through review, simulation and testing techniques to confirm that the I/O data is mapped to the correct application logic.

12.4.6.2 Each application software module shall be checked through review, simulation and testing techniques to determine that the intended function is correctly executed and unintended functions are not executed.

The tests shall be suitable for the specific module being tested and the following shall be considered:

- exercising all parts of the application model;
- exercising data boundaries;
- timing effects due to the sequence of execution;
- proper sequence implementation.

12.4.6.3 The results of the application software module testing shall be available.

12.4.7 Requirements for application software integration testing

NOTE Testing that the software is correctly integrated is a verification activity (see also 12.7).

12.4.7.1 The application software tests shall show that all application software modules and components/subsystems interact correctly with each other and with the underlying embedded software to perform their intended function.

NOTE Il convient que des essais soient également effectués pour confirmer que le logiciel n'exécute pas des fonctions non prévues qui compromettraient ses exigences de sécurité.

12.4.7.2 Les résultats des essais d'intégration du logiciel d'application doivent être disponibles, et doivent:

a) statuer sur les résultats des essais, et

b) déclarer si les objectifs et les critères de la spécification d'essai ont été satisfaits ou non.

En cas de défaillance, les raisons de cette dernière doivent être rapportées.

12.4.7.3 Pendant l'intégration du logiciel d'application, toute modification au logiciel doit faire l'objet d'une analyse d'impact sur la sécurité, qui doit déterminer:

a) tous les modules logiciels touchés, et

b) les activités de reprise de la conception et de vérification à nouveau nécessaires (voir 12.6).

12.5 Intégration du logiciel d'application avec le sous-système du SIS

NOTE Cette phase est la case 12.5 de la Figure 11.

12.5.1 Objectif

12.5.1.1 L'objectif de ce paragraphe est de démontrer que le logiciel d'application répond à sa spécification des exigences concernant la sécurité du logiciel, lorsqu'il est exécuté sur le matériel et le logiciel intégré, utilisés dans le sous-système du SIS.

NOTE Selon la nature de l'application, ces activités peuvent être combinées avec celles mentionnées en 12.4.7.

12.5.2 Exigences

12.5.2.1 Les essais d'intégration doivent être spécifiés aussitôt que possible dans le cycle de vie de sécurité du logiciel, afin d'assurer la compatibilité du logiciel d'application avec la plate-forme du matériel et du logiciel intégré, de telle manière que les exigences de sécurité fonctionnelles et de performances puissent être satisfaites.

NOTE 1 Le domaine d'application des essais peut être réduit sur la base d'une expérience antérieure.

NOTE 2 Il convient que les points suivants soient abordés:

– la division du logiciel d'application en ensembles d'intégration gérables;

– les scénarii d'essai et les données d'essai;

– les types d'essais à exécuter;

– l'environnement d'essai, les outils, la configuration et les programmes;

– les critères d'essai sur lesquels la fin des essais sera jugée; et

– les procédures relatives aux actions correctives lors d'une défaillance pendant l'essai.

12.5.2.2 Pendant les essais, toute modification ou tout changement doit faire l'objet d'une analyse d'impact sur la sécurité, qui doit déterminer:

a) tous les modules logiciels touchés, et

b) les activités de vérification à nouveau nécessaires (voir 12.7).

12.5.2.3 Les informations suivantes, concernant les essais, doivent être disponibles:

a) les éléments de configuration en essai

b) les éléments de configuration supportant l'essai (outils et fonctionnalité externe);

c) le personnel impliqué;

NOTE Tests should also be carried out to confirm that the software does not perform unintended functions that jeopardize its safety requirements.

12.4.7.2 The results of application software integration testing shall be available and shall state

a) the test results; and

b) whether the objectives and criteria of the test specification have been met.

If there is a failure, the reasons for the failure shall be reported.

12.4.7.3 During application software integration, any modification to the software shall be subject to a safety impact analysis that shall determine:

a) all software modules impacted; and

b) the necessary re-design and re-verification activities (see 12.6).

12.5 Integration of the application software with the SIS subsystem

NOTE This phase is box 12.5 of Figure 11.

12.5.1 Objective

12.5.1.1 The objective of this clause is to demonstrate that the application software meets its software safety requirements specification when running on the hardware and embedded software used in the SIS subsystem.

NOTE Depending on the nature of the application, these activities may be combined with 12.4.7.

12.5.2 Requirements

12.5.2.1 Integration tests shall be specified as early in the software safety life cycle as possible to ensure the compatibility of the application software with the hardware and embedded software platform such that the functional and performance safety requirements can be met.

NOTE 1 The scope of the tests may be reduced based on previous experience.

NOTE 2 The following should be addressed:

– the division of the application software into manageable integration sets;

– test cases and test data;

– types of tests to be performed;

– test environment, tools, configuration and programs;

– test criteria on which the completion of the test will be judged; and

– procedures for corrective action on failure during test.

12.5.2.2 During testing, any modification or change shall be subject to a safety impact analysis which shall determine

a) all software modules impacted; and

b) the necessary re-verification activities (see 12.7).

12.5.2.3 The following test information shall be available:

a) configuration items under test;

b) configuration items supporting test (tools and external functionality);

c) personnel involved;

d) les scénarii d'essai et les scripts d'essai;

e) les résultats d'essai;

f) si l'objectif et les critères de l'essai ont été satisfaits ou non, et

g) en cas de défaillance, les raisons de cette dernière, l'analyse de défaillance et les enregistrements relatifs à la correction, comprenant le test et la vérification à nouveau nécessaires (voir 12.5.2.2).

12.6 Procédures de modification du logiciel utilisant le FPL et le LVL

NOTE Le terme modification s'applique principalement aux changements ayant lieu pendant la phase d'exploitation du logiciel.

12.6.1 Objectif

12.6.1.1 Les exigences de ce paragraphe ont pour but d'assurer que le logiciel continue à répondre à la spécification des exigences concernant la sécurité du logiciel après des modifications.

12.6.2 Exigences de modification

12.6.2.1 Les modifications doivent être effectuées en accord avec 5.2.6.2.2, 5.2.7 et l'Article 17, avec les exigences supplémentaires suivantes:

a) avant la modification une analyse des effets de la modification sur la sécurité du processus et sur l'état de la conception du logiciel doit être effectuée et utilisée pour procéder à la modification;

b) la planification de la sécurité relative à la modification et à la vérification à nouveau nécessaire doit être disponible.

c) les modifications et les vérifications à nouveau nécessaires doivent être effectuées selon la planification;

d) la planification relative aux conditions requises pendant la modification et les essais doit être considérée;

e) toute la documentation affectée par la modification doit être mise à jour;

f) les détails concernant toutes les activités de modification du SIS doivent être disponibles (par exemple, un journal).

12.7 Vérification du logiciel d'application

12.7.1 Objectifs

12.7.1.1 Le premier objectif de ce paragraphe est de démontrer que les informations sont satisfaisantes.

12.7.1.2 Le deuxième objectif de ce paragraphe est de démontrer que les résultats de sortie satisfont aux exigences définies pour chaque phase du cycle de vie de sécurité du logiciel d'application.

12.7.2 Exigences

12.7.2.1 La planification de la vérification doit être effectuée pour chaque phase du cycle de vie du logiciel d'application, en accord avec l'Article 7.

12.7.2.2 Les résultats de chaque phase doivent être vérifiés vis-à-vis de:

a) l'adéquation des sorties d'une phase particulière du cycle de vie par rapport aux exigences relatives à cette phase;

d) test cases and test scripts;

e) the test results;

f) whether the objective and criteria of the tests have been met; and

g) if there is a failure, the reasons for the failure, the analysis of the failure and the records of correction including re-test and re-verification (see 12.5.2.2).

12.6 FPL and LVL software modification procedures

NOTE Modification applies primarily to changes occurring during the operational phase of the software.

12.6.1 Objective

12.6.1.1 The objective of the requirements of this clause is to ensure that the software continues to meet the software safety requirements specification after modifications.

12.6.2 Modification requirements

12.6.2.1 Modifications shall be carried out in accordance with 5.2.6.2.2, 5.2.7 and Clause 17 with the following additional requirements.

a) Prior to modification an analysis of the effects of the modification on the safety of the process and on the software design status shall be carried out and used to direct the modification.

b) Safety planning for the modification and re-verification shall be available.

c) Modifications and re-verifications shall be carried out in accordance with the planning.

d) The planning for conditions required during modification and testing shall be considered.

e) All documentation affected by the modification shall be updated.

f) Details of all SIS modification activities shall be available (for example, a log).

12.7 Application software verification

12.7.1 Objectives

12.7.1.1 The first objective of this clause is to demonstrate that the information is satisfactory.

12.7.1.2 The second objective of this clause is to demonstrate that the output results satisfy the defined requirements at each phase of the application software safety life cycle.

12.7.2 Requirements

12.7.2.1 Verification planning shall be carried out for each phase of the application software life cycle in accordance with Clause 7.

12.7.2.2 The results of each phase shall be verified for

a) the adequacy of the outputs from the particular life-cycle phase against the requirements for that phase;

b) l'adéquation de la couverture de la revue, de l'inspection et/ou des essais concernant les sorties;

c) la compatibilité entre les sorties, produites à différentes phases de cycle de vie;

d) l'exactitude des données.

12.7.1.3 Il convient que la vérification traite également les points suivants:

a) la testabilité;

b) la lisibilité:

c) la traçabilité.

NOTE 1 Il convient que le format des données dans le programme d'application soit vérifié en ce qui concerne:

– la complétude (l'intégralité);

– la cohérence intrinsèque;

– la protection contre une altération non autorisée;

– la cohérence avec les exigences fonctionnelles.

NOTE 2 Il convient que les données d'application soient vérifiées en ce qui concerne:

– la cohérence avec les structures des données;

– la complétude (l'intégralité);

– la compatibilité avec le logiciel système de base (par exemple: séquence d'exécution, durée d'exécution, etc.);

– l'exactitude des valeurs des données;

– l'exploitation dans un périmètre de sécurité connu.

NOTE 3 Il convient que les paramètres modifiables soient vérifiés en ce qui concerne la protection contre:

– les valeurs initiales invalides ou non définies;

– les valeurs erronées;

– les modifications non autorisées;

– l'altération (la corruption) des données.

NOTE 4 Il convient que les interfaces de communication, de processus et leurs logiciels associés soient vérifiés, en ce qui concerne:

– la détection des défaillances;

– la protection contre l'altération (la corruption) des messages; et

– la validation des données.

12.7.1.4 Il convient que les fonctions non sécuritaires et les interfaces du processus intégrées avec les signaux et les fonctions de sécurité soient vérifiées, en ce qui concerne:

- la non-interférence avec les fonctions de sécurité;
- la protection contre les interférences avec les fonctions de sécurité dans le cas d'un dysfonctionnement des fonctions non sécuritaires.

13 Essais de recette en usine (FAT)

NOTE Cet article est donné à titre d'information.

13.1 Objectifs

13.1.1 L'objectif des essais de recette en usine (FAT) est de procéder aux essais de l'ensemble unité logique et logiciel associé, pour assurer qu'il satisfait aux exigences définies par la spécification des exigences relatives à la sécurité. Le fait d'essayer l'unité logique et le logiciel associé avant de les installer au sein d'une installation industrielle permet d'identifier et de corriger aisément des erreurs.

NOTE Les essais de recette en usine sont parfois désignés sous le nom d'essais d'intégration et peuvent faire partie de la validation.

b) the adequacy of the review, inspection and/or testing coverage of the outputs;

c) compatibility between outputs generated at different life-cycle phases;

d) correctness of the data.

12.7.2.3 Verification should also address

a) testability;

b) readability;

c) traceability.

NOTE 1 Data format in the application program should be verified for

– completeness;

– self-consistency;

– protection against unauthorized alteration;

– consistency with the functional requirements.

NOTE 2 Application data should be verified for

– consistency with the data structures;

– completeness;

– compatibility with the underlying system software (for example, sequence of execution, run-time);

- correct data values;

- operation within a known safe boundary.

NOTE 3 Modifiable parameters should be verified for protection against

- invalid of undefined initial values;

- erroneous values;

- unauthorized changes;

- data corruption.

NOTE 4 Communications, process interfaces and associated software should be verified for

– failure detection;

– protection against message corruption, and

– data validation.

12.7.2.4 Non-safety functions and process interfaces integrated with safety related signals and functions should be verified for

- non-interference with the safety functions;
- protection against interference with the safety functions in the case of malfunction of the non-safety functions.

13 Factory acceptance testing (FAT)

NOTE This clause is informative.

13.1 Objectives

13.1.1 The objective of a factory acceptance test (FAT) is to test the logic solver and associated software together to ensure it satisfies the requirements defined in the safety requirement specification. By testing the logic solver and associated software prior to installing in a plant, errors can be readily identified and corrected.

NOTE The factory acceptance test is sometimes referred to as an integration test and can be part of the validation.

13.2 Recommandations

13.2.1 Il convient que la nécessité de recourir aux essais de recette en usine (FAT) soit spécifiée pendant la phase de conception d'un projet.

NOTE 1 Une collaboration étroite entre le fournisseur de l'unité logique et le contractant responsable de la conception peut être requise afin de mettre au point les essais d'intégration.

NOTE 2 Ces activités suivent les phases de conception et de développement et précèdent l'installation et la mise en service.

NOTE 3 Ces activités sont applicables aux sous-systèmes d'un SIS, avec ou sans l'électronique programmable.

NOTE 4 Il est habituel que les essais de recette en usine (FAT) aient lieu dans un environnement d'usine avant l'installation et la mise en service à l'usine.

13.2.2 Il convient que la planification des essais de recette en usine (FAT) spécifie les points suivants:

- le type des essais à exécuter, comprenant les essais de fonctionnalité du système «boîte-noire» (c'est-à-dire, méthode de conception des essais qui traite le système comme une «boîte-noire», ainsi la connaissance explicite de sa structure interne n'est pas utilisée. La conception des essais «boîte-noire» est habituellement décrite comme se concentrant sur les exigences d'essai de fonction. Des synonymes de «boîte-noire» sont: essais comportementaux, fonctionnels, en boîte-opaque, et en boîte-fermée); essais de qualité de fonctionnement (synchronisation, fiabilité et disponibilité, intégrité, cibles de sécurité et contraintes), essais environnementaux (y compris, CEM, essais de durée de vie et de contraintes), essais d'interfaces, essais en modes dégradés et/ou d'anomalie, essais des exceptions, application des manuels de maintenance et d'exploitation du SIS;
- les scénarii d'essai, les descriptions des essais et les données d'essai;

  NOTE Il est très important de dire clairement qui est responsable du développement du scénario d'essai, qui va être responsable de l'exécution de l'essai et qui va être témoin de l'essai.
- la dépendance à l'égard des autres systèmes/interfaces;
- l'environnement d'essai et les outils;
- la configuration de l'unité logique;
- les critères d'essai sur lesquels la fin des essais doit être jugée;
- les procédures relatives aux actions correctives lors d'une défaillance pendant l'essai.
- les compétences du personnel d'essai;
- la localisation physique.

NOTE Les essais ne pouvant pas être physiquement effectués, sont normalement traités par un argumentaire formel montrant pourquoi le SIS satisfait à la prescription, la cible ou la contrainte.

13.2.3 Il convient que les essais de recette en usine (FAT) aient lieu sur une version définie de l'unité logique.

13.2.4 Il convient que les essais de recette en usine (FAT) soient conduits selon la planification de ces derniers. Il convient que ces essais montrent que toute la logique s'exécute correctement.

13.2.5 Pour chaque essai effectué, il convient que les points suivants soient traités:

- la version de la planification d'essai qui a été utilisée;
- la caractéristique de la fonction instrumentée de sécurité et les performances objet de l'essai;
- les procédures d'essai détaillées et les descriptions des essais;
- l'enregistrement chronologique des activités d'essai;
- les outils, les équipements et les interfaces utilisés.

13.2 Recommendations

13.2.1 The need for a FAT should be specified during the design phase of a project.

NOTE 1 Close co-operation between the logic solver supplier and design contractor may be required in order to develop the integration tests.

NOTE 2 The activities follow the design and development phases and precede the installation and commissioning.

NOTE 3 The activities are applicable to the subsystems of an SIS with or without programmable electronics.

NOTE 4 It is usual for the FAT to take place in a factory environment prior to installation and commissioning in the plant.

13.2.2 The planning for a FAT should specify the following

- Types of tests to be performed including black-box system functionality tests (i.e., test design method that treats the system as a “black box”, so it does not explicitly use knowledge of its internal structure. Black-box test design is usually described as focusing on testing function requirements. Synonyms for black box include behavioural, functional, opaque-box, and closed-box testing); performance tests (timing, reliability and availability, integrity, safety targets and constraints), environmental tests (including EMC, life- and stress-testing), interface testing, testing in degraded and/or fault modes, exception testing, application of the SIS maintenance and operating manuals.
- Test cases, test description and test data.

  NOTE It is very important to make clear who is responsible for developing the test case and who is going to be responsible for carrying out the test and witnessing the test.
- Dependence on other systems/interfaces.
- Test environment and tools.
- Logic solver configuration.
- Test criteria on which the completion of the test shall be judged.
- Procedures for corrective action on failure of test.
- Test personnel competences.
- Physical location.

NOTE For tests that cannot be physically demonstrated, these are normally resolved by a formal argument as to why the SIS achieves the requirement, target or constraint.

13.2.3 FAT should take place on a defined version of the logic solver.

13.2.4 The FAT should be conducted in accordance with the FAT planning. These tests should show that all the logic performs correctly.

13.2.5 For each test carried out the following should be addressed:

- the version of the test planning being used;
- the safety instrumented function and performance characteristic being tested;
- the detailed test procedures and test descriptions;
- a chronological record of the test activities;
- the tools, equipment and interfaces used.

13.2.6 Il convient que les résultats des FAT soient documentés, en mentionnant:

a) les scénarii d'essai;

b) les résultats d'essai, et

c) si les objectifs et les critères d'essai ont été satisfaits ou non. En cas de défaillance pendant l'essai, il convient que les raisons de cette dernière soient documentées et analysées, et que l'action corrective appropriée soit mise en oeuvre.

13.2.7 Pendant les FAT, il convient que toute modification ou changement soit soumis à une analyse de sécurité pour déterminer:

a) l'ampleur de l'impact sur chaque fonction instrumentée de sécurité, et

b) l'étendue du contre-essai qu'il convient de définir et de mettre en oeuvre.

NOTE En fonction des résultats des FAT, la mise en service peut commencer alors que l'action corrective est entreprise.

14 Installation et mise en service du SIS

14.1 Objectifs

14.1.1 Les objectifs des exigences de cet article sont:

- installer le système instrumenté de sécurité selon les spécifications et les plans;
- mettre en service·le système instrumenté de sécurité de manière à ce qu'il soit prêt pour la validation finale du système.

14.2 Exigences

14.2.1 La planification de l'installation et de la mise en service doit définir toutes les activités requises pour l'installation et la mise en service. Elle doit être conforme à cette norme, en fournissant les informations suivantes:

- les activités d'installation et de mise en service;
- les procédures, les mesures et les techniques à utiliser pour l'installation et la mise en service;
- le moment où ces activités doivent avoir lieu dans le temps;
- les personnes, les services et les organisations responsables de ces activités.

Le cas échéant, la planification de l'installation et de la mise en service peut être intégrée dans la planification globale du projet.

14.2.2 Tous les composants du système instrumenté de sécurité doivent être correctement installés, en respectant le(s) plan(s) de conception et d'installation (voir 14.2.1).

14.2.3 Le système instrumenté de sécurité doit être mis en service en accord avec la planification, en vue de la validation finale du système. Les activités de mise en service doivent inclure, mais ne doivent pas être limitée à, la confirmation des points suivants:

- la mise à la terre (la mise au conducteur de protection) a été correctement raccordée;
- les sources d'énergie ont été correctement connectées et sont opérationnelles;
- les dispositifs de blocage pour le transport et des matériaux d'emballage ont été retirés;
- aucun dommage physique n'est constaté;
- tous les instruments ont été correctement étalonnés;
- tous les dispositifs sur le terrain sont opérationnels;

13.2.6 The results of FAT should be documented, stating

a) the test cases;

b) the test results; and

c) whether the objectives and criteria of the test criteria have been met.

If there is a failure during test, the reasons for the failure should be documented and analysed and the appropriate corrective action should be implemented.

13.2.7 During FAT, any modification or change should be subject to a safety analysis to determine

a) the extent of impact on each safety instrumented function; and

b) the extent of re-test which should be defined and implemented.

NOTE Commissioning may commence whilst corrective action is undertaken, depending on the results of the FAT.

14 SIS installation and commissioning

14.1 Objectives

14.1.1 The objectives of the requirements of this clause are to

- install the safety instrumented system according to the specifications and drawings;
- commission the safety instrumented system so that it is ready for final system validation.

14.2 Requirements

14.2.1 Installation and commissioning planning shall define all activities required for installation and commissioning. The planning shall provide the following:

- the installation and commissioning activities;
- the procedures, measures and techniques to be used for installation and commissioning;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities.

Installation and commissioning planning may be integrated in the overall project planning where appropriate.

14.2.2 All safety instrumented system components shall be properly installed according to the design and installation plan(s) (see 14.2.1).

14.2.3 The safety instrumented system shall be commissioned in accordance with planning in preparation for the final system validation. Commissioning activities shall include, but not be limited to, confirmation of the following:

- earthing (grounding) has been properly connected;
- energy sources have been properly connected and are operational;
- transportation stops and packing materials have been removed;
- no physical damage is present;
- all instruments have been properly calibrated;
- all field devices are operational;

- l'unité logique et les entrées/sorties sont opérationnelles;
- les interfaces vers d'autres systèmes et périphériques sont opérationnelles.

14.2.4 Des enregistrements appropriés de la mise en service du SIS doivent être produits, mentionner les résultats des essais et si les objectifs et les critères identifiés pendant la phase de conception ont été satisfaits ou non. En cas de défaillance, les raisons de cette dernière doivent être enregistrées.

14.2.5 Dans le cas où il a été établi que l'installation réelle n'est pas conforme aux informations de conception, les différences doivent alors être évaluées par une personne compétente et l'impact probable sur la sécurité doit être déterminé. S'il est établi que les différences n'ont aucun impact sur la sécurité, les informations de conception doivent alors être mises à jour suivant l'état «conforme à l'exécution». Si les différences ont un impact négatif sur la sécurité, l'installation doit alors être modifiée pour satisfaire aux exigences de conception.

15 Validation de sécurité du SIS

15.1 Objectif

15.1.1 L'objectif des exigences de cet article est de valider, par inspection et essais, que le système instrumenté de sécurité installé et mis en service, ainsi que ses fonctions instrumentées de sécurité associées, répondent effectivement aux exigences, comme cela est indiqué dans la spécification des exigences concernant la sécurité.

NOTE Ceci est parfois désigné par «essai de recette sur site» (SAT).

15.2 Exigences

15.2.1 La planification de la validation du SIS doit définir toutes les activités requises pour la validation. Les points suivants doivent être inclus:

- les activités de validation, incluant la validation du (des) système(s) instrumenté(s) de sécurité, par rapport à la spécification des exigences concernant la sécurité, y compris la mise en oeuvre et la résolution des recommandations qui en découlent;
- la validation de tous les modes de fonctionnement appropriés du processus et de ses équipements associés comprenant:
  - — la préparation pour l'utilisation, comprenant l'initialisation et le réglage;
  - — le fonctionnement au démarrage; en automatique; en manuel; en semi-automatique; en régime établi;
  - — la réinitialisation; l'arrêt; la maintenance;
  - — les conditions anormales raisonnablement prévisibles, par exemple, celles identifiées par la phase d'analyse de risque.
- les procédures, les mesures et les techniques à utiliser pour la validation;
- le moment où ces activités doivent avoir lieu dans le temps;
- les personnes, les services et les organisations responsables de ces activités, et les niveaux d'indépendance pour les activités de validation;
- la référence aux informations par rapport auxquelles la validation doit être effectuée (par exemple, diagramme de cause et d'effet).

NOTE 1 Des exemples d'activités de validation sont: les essais en boucle, les procédures d'étalonnage, la simulation du logiciel d'application.

- logic solver and input/outputs are operational;
- the interfaces to other systems and peripherals are operational.

14.2.4 Appropriate records of the commissioning of the SIS shall be produced, stating the test results and whether the objectives and criteria identified during the design phase have been met. If there is a failure, the reasons for the failure shall be recorded.

14.2.5 Where it has been established that the actual installation does not conform to the design information then the difference shall be evaluated by a competent person and the likely impact on safety determined. If it is established that the difference has no impact on safety, then the design information shall be updated to "as-built" status. If the difference has a negative impact on safety, then the installation shall be modified to meet the design requirements.

15 SIS safety validation

15.1 Objective

15.1.1 The objective of the requirements of this clause is to validate, through inspection and testing, that the installed and commissioned safety instrumented system and its associated safety instrumented functions achieve the requirements as stated in the safety requirement specification.

NOTE This is sometimes referred to as a site acceptance test (SAT).

15.2 Requirements

15.2.1 Validation planning of the SIS shall define all activities required for validation. The following items shall be included**.**

- The validation activities including validation of the safety instrumented system(s) with respect to the safety requirements specification including implementation and resolution of resulting recommendations.
- Validation of all relevant modes of operation of the process and its associated equipment including
  - preparation for use including setting and adjustment;
  - start-up, automatic, manual, semi-automatic, steady state of operation;
  - re-setting, shutdown, maintenance;
  - reasonably foreseeable abnormal conditions, for example, those identified through the risk analysis phase;
- the procedures, measures and techniques to be used for validation;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities and levels of independence for validation activities;
- reference to information against which validation shall be carried out (for example, cause and effect chart).

NOTE Examples of validation activities include loop testing, calibration procedures, simulation of application software.

15.2.2 Une planification supplémentaire de la validation relative au logiciel d'application de sécurité doit inclure les points suivants:

a) l'identification du logiciel de sécurité qui nécessite d'être validé pour chaque mode d'exploitation du processus, avant de commencer la mise en service;

b) les informations relatives à la stratégie technique concernant la validation comprenant;

   — les techniques manuelles et automatisées;

   — les techniques statiques et dynamiques;

   — les techniques analytiques et statistiques;

c) conformément à b), les mesures (techniques) et les procédures qui doivent être utilisées pour confirmer que chaque fonction instrumentée de sécurité est conforme aux exigences spécifiées concernant les fonctions instrumentées de sécurité du logiciel (voir 12.2), et aux exigences spécifiées concernant l'intégrité de sécurité du logiciel (voir 12.2);

d) l'environnement requis dans lequel les activités de validation doivent avoir lieu (par exemple pour les essais, celui-ci inclurait des outils et des équipements étalonnés);

e) les critères d'acceptation/de refus pour réaliser la validation du logiciel comprenant:

   — le processus requis et les signaux d'entrée de l'opérateur avec leurs séquences et leurs valeurs;

   — les signaux de sortie prévus avec leurs séquences et leurs valeurs; et

   — d'autres critères d'acceptation, par exemple, l'utilisation de la mémoire, la synchronisation et les tolérances de valeur;

f) les règles et les procédures concernant l'évaluation des résultats de la validation, traitant en particulier des défaillances.

NOTE Ces exigences sont basées sur les exigences générales de 12.2.

15.2.3 Dans le cas où la précision de mesure est requise en tant qu'élément de la validation, il convient que les instruments utilisés pour cette fonction soient étalonnés en référence à une spécification se rapportant à une norme, dans les limites d'une incertitude appropriée à l'application. Si cet étalonnage n'est pas réalisable, une autre méthode doit être utilisée et documentée.

15.2.4 La validation du système instrumenté de sécurité et de ses fonctions instrumentées de sécurité associées doit être effectuée selon la planification de la validation du système instrumenté de sécurité. Les activités de validation doivent inclure les points suivants, sans toutefois devoir être limitées à ces derniers:

- le système instrumenté de sécurité fonctionne sous des modes de fonctionnement normaux et anormaux (par exemple, démarrage, arrêt), tels qu'ils sont identifiés dans la spécification des exigences concernant la sécurité;
- la confirmation que l'interaction défavorable du système de commande de processus de base et d'autres systèmes liés, n'affectent pas l'exploitation correcte du système instrumenté de sécurité;
- le système instrumenté de sécurité communique correctement (le cas échéant) avec le système de commande de processus de base ou avec tout autre système ou réseau;
- les capteurs, l'unité logique et les éléments terminaux fonctionnent selon la spécification des exigences concernant la sécurité, y compris tous les canaux redondants;

  NOTE Si un essai de recette en usine (FAT) est réalisé sur l'unité logique, comme cela est décrit à l'Article 13, la validation de l'unité logique par le FAT peut être prise en compte.

- la documentation du système instrumenté de sécurité est cohérente avec le système installé;
- la confirmation que la fonction instrumentée de sécurité fonctionne comme cela est spécifié pour des valeurs de variables du processus invalides (par exemple, hors gamme);

15.2.2 Additional validation planning for the safety application software shall include the following.

a) Identification of the safety software which needs to be validated for each mode of process operation before commissioning commences.

b) Information on the technical strategy for the validation including
   - manual and automated techniques;
   - static and dynamic techniques;
   - analytical and statistical techniques.

c) In accordance with b), the measures (techniques) and procedures that shall be used for confirming that each safety instrumented function conforms with the specified requirements for the software safety instrumented functions (see 12.2) and the specified requirements for software safety integrity (see 12.2).

d) The required environment in which the validation activities are to take place (for example, for tests this would include calibrated tools and equipment).

e) The pass/fall criteria for accomplishing software validation including:
   - the required process and operator input signals with their sequences and their values;
   - the anticipated output signals with their sequences and their values; and
   - other acceptance criteria, for example, memory usage, timing and value tolerances.

f) The policies and procedures for evaluation the results of the validation, particularly failures.

NOTE These requirements are based on the general requirements of 12.2.

15.2.3 Where measurement accuracy is required as part of the validation then instruments used for this function should be calibrated against a specification traceable to a standard within an uncertainty appropriate to the application. If such a calibration is not feasible, an alternative method shall be used and documented.

15.2.4 The validation of the safety instrumented system and its associated safety instrumented functions shall be carried out in accordance with the safety instrumented system validation planning. Validation activities shall include, but not be limited to, the following:

- the safety instrumented system performs under normal and abnormal operating modes (for example, start-up, shutdown) as identified in the safety requirement specification;
- confirmation that adverse interaction of the basic process control system and other connected systems do not affect the proper operation of the safety instrumented system;
- the safety instrumented system properly communicates (where required) with the basic process control system or any other system or network;
- sensors, logic solver, and final elements perform in accordance with the safety requirement specification, including all redundant channels;

  NOTE If a factory acceptance test (FAT) was performed on the logic solver as described in Clause 13, credit may be taken for validation of the logic solver by the FAT.

- safety instrumented system documentation is consistent with the installed system;
- confirmation that the safety instrumented function performs as specified on invalid process variable values (for example, out of range);

- la séquence d'arrêt correcte est activée;
- le système instrumenté de sécurité donne une signalisation et un affichage de fonctionnement appropriés;
- les calculs qui sont inclus dans le système instrumenté de sécurité sont corrects;
- les fonctions de réinitialisation du système instrumenté de sécurité fonctionnent comme cela est défini par la spécification des exigences concernant la sécurité;
- les fonctions de dérivation fonctionnent correctement;
- les annulations prioritaires de démarrages fonctionnent correctement;
- les systèmes d'arrêt manuel fonctionnent correctement;
- les intervalles des tests périodiques sont documentés dans les procédures de maintenance;
- les fonctions d'alarme de diagnostic fonctionnent comme cela est demandé;
- la confirmation que le système instrumenté de sécurité se comporte comme cela est demandé lors d'une perte d'alimentation (par exemple, alimentation électrique, air, hydraulique) et la confirmation que, lorsque les alimentations sont rétablies, le système instrumenté de sécurité revient à l'état souhaité;
- la confirmation que l'immunité CEM a été obtenue, comme cela a été prescrit par la spécification des exigences concernant la sécurité (voir 10.3).

15.2.5 La validation du logiciel doit montrer que toutes les exigences de sécurité du logiciel spécifiées sont correctement remplies (voir 12.2), et que le logiciel ne compromet pas les exigences de sécurité dans des conditions d'anomalie du SIS et dans des modes de fonctionnement dégradés ou en exécutant une fonctionnalité du logiciel non définie dans la spécification. Les informations des activités de validation doivent être disponibles.

15.2.6 Les informations ad hoc des résultats de la validation du SIS doivent être données et traiter de:

- la version de la planification de la validation du SIS qui a été utilisée;
- la fonction instrumentée de sécurité en essais (ou en analyse), avec la référence spécifique à la prescription identifiée lors de la planification de la validation du SIS;
- les outils et les équipements utilisés, avec les données d'étalonnage;
- les résultats de chaque essai;
- la version de la spécification d'essai qui a été utilisée;
- les critères d'acceptation des essais d'intégration;
- la version du matériel et du logiciel du SIS qui ont été essayés;
- toute divergence entre les résultats attendus et les résultats réels;
- l'analyse faite et les décisions prises quant à savoir, dans le cas où des divergences apparaissent, si l'essai peut continuer ou au contraire si une demande de modification doit être émise.

15.2.7 Lorsque des divergences apparaissent entre les résultats attendus et les résultats réels, l'analyse faite et les décisions relatives à la poursuite de la validation, ou à l'émission d'une demande de modification et à la nécessité de revenir à une étape antérieure du cycle de vie du développement, toutes ces informations doivent être disponibles et faire partie des résultats de la validation de sécurité du logiciel.

- the proper shutdown sequence is activated;
- the safety instrumented system provides the proper annunciation and proper operation display;
- computations that are included in the safety instrumented system are correct;
- the safety instrumented system reset functions perform as defined in the safety requirement specification;
- bypass functions operate correctly;
- start-up overrides operate correctly;
- manual shutdown systems operate correctly;
- the proof-test intervals are documented in the maintenance procedures;
- diagnostic alarm functions perform as required;
- confirmation that the safety instrumented system performs as required on loss of utilities (for example, electrical power, air, hydraulics) and confirmation that, when the utilities are restored, the safety instrumented system returns to the desired state;
- confirmation that the EMC immunity, as specified in the safety requirements specification (see 10.3), has been achieved.

15.2.5 The software validation shall show that all of the specified software safety requirements (see 12.2) are correctly performed, and the software does not jeopardize the safety requirements under SIS fault conditions and in degraded modes of operation or by executing software functionality not defined in the specification. The information of the validation activities shall be available.

15.2.6 Appropriate information of the results of the SIS validation shall be produced which provides

- the version of the SIS validation planning being used;
- the safety instrumented function under test (or analysis), along with the specific reference to the requirement identified during SIS validation planning;
- tools and equipment used, along with calibration data;
- the results of each test;
- the version of the test specification used;
- the criteria for acceptance of the integration tests;
- the version of the SIS hardware and software being tested;
- any discrepancy between expected and actual results;
- the analysis made and the decisions taken on whether to continue the test or issue a change request, in the case where discrepancies occur.

15.2.7 When discrepancies occur between expected and actual results, the analysis made and the decisions taken on whether to continue the validation or to issue a change request and return to an earlier part of the development life cycle, shall be available as part of the results of the safety validation.

15.2.8 Après la validation du système instrumenté de sécurité et avant que les dangers identifiés ne soient présents, les activités suivantes doivent être conduites:

- toutes les fonctions de dérivation (par exemple, unité logique de PE et forçages de capteur de PE, alarmes désactivées) doivent être revenues à leur position normale;
- toutes les vannes d'isolement du processus doivent être paramétrées selon les exigences et les procédures du processus au démarrage;
- tous les matériaux d'essai (par exemple, fluides) doivent être éliminés;
- tous les forçages doivent être retirés et le cas échéant, toutes les autorisations de forçage doivent être inhibées.

16 Exploitation et maintenance du SIS

16.1 Objectifs

16.1.1 Les objectifs des exigences de cet article sont de:

- d'assurer que le SIL requis de chaque fonction instrumentée de sécurité est maintenu pendant l'exploitation et la maintenance;
- exploiter et maintenir le SIS de sorte que la sécurité fonctionnelle à la conception soit maintenue.

16.2 Exigences

16.2.1 L'exploitation et la planification de la maintenance du système instrumenté de sécurité doivent être effectuées. Elles doivent traiter les points suivants:

- les activités d'exploitation périodique et anormale;
- les activités de tests périodiques, de maintenance préventive et de dépannage;
- les procédures, les mesures et les techniques à utiliser pour l'exploitation et la maintenance;
- la vérification de l'adéquation aux procédures d'exploitation et de maintenance;
- le moment où ces activités doivent avoir lieu dans le temps;
- les personnes, les services et les organisations responsables de ces activités.

16.2.2 Les procédures d'exploitation et de maintenance doivent être développées en accord avec la planification de la sécurité ad hoc et doivent fournir les informations suivantes:

- les actions périodiques qui doivent être effectuées afin de maintenir la sécurité fonctionnelle du SIS «comme à la conception», par exemple, adhérer aux intervalles des tests périodiques définis par la détermination du SIL;
- les actions et les contraintes nécessaires pour prévenir un état de non-sécurité et/ou pour réduire les conséquences d'un événement dangereux pendant la maintenance ou l'exploitation (par exemple, lorsqu'un système doit être dérivé (shunté) pour les essais ou la maintenance, quelles étapes supplémentaires d'atténuation nécessitent d'être mises en oeuvre);
- les informations qui nécessitent d'être maintenues lors d'une défaillance du système et les taux de sollicitation sur le SIS;
- les informations qui nécessitent d'être maintenues, montrant les résultats des audits et des essais effectués sur le SIS;
- les procédures de maintenance à suivre lorsque des anomalies ou des défaillances ont lieu dans le SIS, incluant:

15.2.8 After the safety instrumented system validation and prior to the identified hazards being present, the following activities shall be carried out.

- All bypass functions (for example, PE logic solver and PE sensor forces, disabled alarms) shall be returned to their normal position.
- All process isolation valves shall be set according to the process start-up requirements and procedures.
- All test materials (for example, fluids) shall be removed.
- All forces shall be removed and if applicable all force enables shall be removed.

16 SIS operation and maintenance

16.1 Objectives

16.1.1 The objectives of the requirements of this clause are:

- to ensure that the required SIL of each safety instrumented function is maintained during operation and maintenance;
- to operate and maintain the SIS so that the designed functional safety is maintained.

16.2 Requirements

16.2.1 Operation and maintenance planning for the safety instrumented system shall be carried out. It shall provide the following:

- routine and abnormal operation activities;
- proof testing, preventive and breakdown maintenance activities;
- the procedures, measures and techniques to be used for operation and maintenance;
- verification of adherence to operations and maintenance procedures;
- when these activities shall take place;
- the persons, departments and organizations responsible for these activities.

16.2.2 Operation and maintenance procedures shall be developed in accordance with the relevant safety planning and shall provide the following:

- the routine actions which need to be carried out to maintain the "as designed" functional safety of the SIS, for example, adhering to proof-test intervals defined by the SIL determination;
- the actions and constraints that are necessary to prevent an unsafe state and/or reduce the consequences of a hazardous event during maintenance or operation (for example, when a system needs to be bypassed for testing or maintenance, what additional mitigation steps need to be implemented);
- the information which needs to be maintained on system failure and demand rates on the SIS;
- the information which needs to be maintained showing results of audits and tests on the SIS;
- the maintenance procedures to be followed when faults or failures occur in the SIS, including

— les procédures de diagnostic et de réparation des anomalies;

— les procédures de revalidation;

— les exigences relatives au compte rendu de maintenance;

— les procédures pour suivre l'exécution de maintenance.

NOTE Ces considérations incluent:

– les procédures de compte rendu de défaillances;

– les procédures d'analyse de défaillances systématiques.

- l'assurance que les équipements d'essai utilisés pendant des activités normales de maintenance sont correctement étalonnés et maintenus.

16.2.3 L'exploitation et la maintenance doivent être mises en oeuvre conformément aux procédures s'y référant.

16.2.4 Les opérateurs doivent être formés à la fonction et à l'exploitation du SIS, et dans leur domaine de compétence. Cette formation doit assurer:

- la compréhension du fonctionnement du SIS (les points déclenchement et l'action résultante qui est prise par le SIS);
- le danger contre lequel le SIS protège;
- l'explication du fonctionnement de tous les commutateurs de dérivation et dans quelles circonstances ces dérivations sont à utiliser;
- l'explication du fonctionnement de tous les commutateurs d'arrêt manuel, des activités de démarrage manuel et dans quelles circonstances ces commutateurs manuels sont à activer;

NOTE Ceci peut inclure la «réinitialisation du système» et le «redémarrage du système».

- l'explication de la conduite à tenir lors de l'activation d'une alarme de diagnostic quelconque (par exemple, quelle mesure doit être prise lorsqu'une alarme du SIS est activée, indiquant qu'il y a un problème avec ce dernier).

16.2.5 Le personnel de maintenance doit être formé de manière adéquate pour entretenir les performances fonctionnelles globales du SIS (matériel et logiciel) à leurs niveaux d'intégrité souhaités.

16.2.6 Les divergences entre le comportement attendu et le comportement réel du SIS doivent être analysées et, en cas de besoin, des modifications doivent être faites, de telle manière que la sécurité prescrite soit maintenue. Ceci doit inclure la surveillance des points suivants:

- les actions prises après une sollicitation sur le système;
- les défaillances des équipements faisant partie du SIS, établies pendant les essais périodiques ou la sollicitation réelle;
- la cause des sollicitations;
- la cause des faux déclenchements.

NOTE Il est très important que TOUTES les divergences entre le comportement attendu et le comportement réel soient analysées. Il convient que celles-ci ne soient pas confondues avec les sollicitations de surveillance rencontrées pendant l'exploitation normale.

16.2.7 Les procédures d'exploitation et de maintenance peuvent nécessiter d'être révisées, si besoin, suivant:

- des audits de la sécurité fonctionnelle;
- des essais sur le SIS.

– procedures for fault diagnostics and repair;
– procedures for revalidation;
– maintenance reporting requirements;
– procedures for tracking maintenance performance.

NOTE Considerations include
– procedures for reporting failures;
– procedures for analysing systematic failures.

- ensuring that test equipment used during normal maintenance activities is properly calibrated and maintained.

16.2.3 Operation and maintenance shall proceed in accordance with the relevant procedures.

16.2.4 Operators shall be trained on the function and operation of the SIS in their area. This training shall ensure the following:

- they understand how the SIS functions (trip points and the resulting action that is taken by the SIS);
- the hazard the SIS is protecting against;
- the operation of all bypass switches and under what circumstances these bypasses are to be used;
- the operation of any manual shutdown switches and manual start-up activity and when these manual switches are to be activated;

  NOTE This may include “system reset” and “system restart”.

- expectation on activation of any diagnostic alarms (for example, what action shall be taken when any SIS alarm is activated indicating there is a problem with the SIS).

16.2.5 Maintenance personnel shall be trained as required to sustain full functional performance of the SIS (hardware and software) to its targeted integrity.

16.2.6 Discrepancies between expected behaviour and actual behaviour of the SIS shall be analysed and, where necessary, modifications made such that the required safety is maintained. This shall include monitoring the following:

- the actions taken following a demand on the system;
- the failures of equipment forming part of the SIS established during routine testing or actual demand;
- the cause of the demands;
- the cause of false trips.

NOTE It is very important that ALL discrepancies between expected behaviour and actual behaviour are analysed. This should not be confused with monitoring demands encountered during normal operation.

16.2.7 The operation and maintenance procedures may require revision, if necessary, following

- functional safety audits;
- tests on the SIS.

16.2.8 Des méthodes d'essais périodiques écrites doivent être développées pour que chaque SIF puisse révéler des défaillances dangereuses non détectées par les diagnostics. Ces méthodes d'essais écrites doivent décrire chaque étape qui est à exécuter et doivent inclure:

- le fonctionnement correct de chaque capteur et élément terminal;
- l'action logique correcte;
- les signalisations et les alarmes correctes.

NOTE Les méthodes suivantes peuvent être utilisées pour déterminer les défaillances non détectées, nécessitant d'être examinées:

– examen des arbres de pannes;

– analyse des modes de défaillance et de leurs effets;

– maintenance basée sur la fiabilité.

16.3 Tests périodiques et inspection

16.3.1 Tests périodiques

16.3.1.1 Les essais périodiques probatoires doivent être conduits en utilisant une procédure écrite (voir 16.2.8) afin de révéler les anomalies non détectées qui empêchent le SIS de fonctionner selon la spécification des exigences concernant la sécurité.

16.3.1.2 Le SIS dans son ensemble doit être essayé, y compris le(s) capteur(s), l'unité logique et le(s) élément(s) terminal(aux) (par exemple, les vannes d'arrêt et les moteurs).

16.3.1.3 La fréquence des essais périodiques doit être celle qui a été décidée en utilisant le calcul PFDavg.

NOTE Les différentes parties du SIS peuvent nécessiter différents intervalles d'essai, par exemple, l'unité logique peut avoir besoin d'un intervalle d'essai différent des capteurs ou des éléments terminaux.

16.3.1.4 Toutes les insuffisances trouvées pendant les essais périodiques doivent être réparées d'une façon sûre et rapide.

16.3.1.5 Périodiquement (intervalle déterminé par l'utilisateur), la fréquence de l'essai doit être réévaluée, sur la base de divers facteurs, comprenant des données d'essais antérieures, une expérience en usine, la dégradation du matériel et la fiabilité du logiciel.

16.3.1.6 Toute modification apportée à la logique de l'application nécessite des essais périodiques complets. Des exceptions sont permises, si une revue appropriée et des essais partiels portant sur les modifications sont faits pour assurer que ces dernières ont été correctement mises en oeuvre.

16.3.2 Inspection

Chaque SIS doit être périodiquement inspecté visuellement pour assurer qu'il n'y a aucune modification non autorisée et aucune détérioration observable (par exemple, boulons ou capots d'instrument manquants, ferrures rouillées, fils ouverts, conduits cassés, câble chauffant cassé et isolation manquante).

16.3.3 Documentation des essais périodiques et de l'inspection

L'utilisateur doit conserver les enregistrements qui certifient que les essais périodiques et les inspections ont été réalisés comme cela est demandé. Ces enregistrements doivent inclure, au minimum, les informations suivantes:

16.2.8 Written proof-test procedures shall be developed for every SIF to reveal dangerous failures undetected by diagnostics. These written test procedures shall describe every step that is to be performed and shall include

- the correct operation of each sensor and final element;
- correct logic action;
- correct alarms and indications.

NOTE The following methods may be used to determine the undetected failures that need to be tested:

– examination of fault trees;

– failure mode and effect analysis;

– reliability centred maintenance.

16.3 Proof testing and inspection

16.3.1 Proof testing

16.3.1.1 Periodic proof tests shall be conducted using a written procedure (see 16.2.8) to reveal undetected faults that prevent the SIS from operating in accordance with the safety requirement specification.

16.3.1.2 The entire SIS shall be tested including the sensor(s), the logic solver and the final element (s) (for example, shutdown valves and motors).

16.3.1.3 The frequency of the proof tests shall be as decided using the PFD_{avg} calculation.

NOTE Different parts of the SIS may require different test intervals, for example, the logic solver may require a different test interval than the sensors or final elements.

16.3.1.4 Any deficiencies found during the proof testing shall be repaired in a safe and timely manner.

16.3.1.5 At some periodic interval (determined by the user), the frequency of testing shall be re-evaluated based on various factors including historical test data, plant experience, hardware degradation, and software reliability.

16.3.1.6 Any change to the application logic requires full proof testing. Exceptions to this are allowed if appropriate review and partial testing of changes are carried out to ensure the changes were correctly implemented.

16.3.2 Inspection

Each SIS shall be periodically visually inspected to ensure there are no unauthorized modifications and no observable deterioration (for example, missing bolts or instrument covers, rusted brackets, open wires, broken conduits, broken heat tracing, and missing insulation).

16.3.3 Documentation of proof tests and inspection

The user shall maintain records that certify that proof tests and inspections were completed as required. These records shall include the following information as a minimum:

a) la description des essais et des inspections effectuées;

b) les dates des essais et des inspections;

c) le nom de la (des) personne(s) qui a (ont) effectué les essais et les inspections;

d) le numéro de série ou tout autre identifiant unique du système essayé (par exemple, numéro de ligne, numéro d'étiquette, numéro d'équipement et numéro de SIF);

e) les résultats des essais et de l'inspection (par exemple, conditions «tel quel»et «en l'état»).

17 Modification du SIS

17.1 Objectifs

17.1.1 Les objectifs des exigences de cet article sont:

- assurer que les modifications à tout système instrumenté de sécurité sont correctement planifiées, revues et approuvées avant de procéder à la modification; et
- assurer que l'intégrité de sécurité du SIS prescrite est maintenue en dépit de toutes les modifications faites à ce dernier.

NOTE Il convient que les modifications au BPCS, à d'autres équipements, au processus ou aux conditions d'exploitation soient passées en revue, afin de déterminer si elles sont telles que la nature ou la fréquence des sollicitations vis-à-vis du SIS est affectée ou non. Il convient que celles qui ont un effet nuisible soient considérées ultérieurement, afin de déterminer si le niveau de la réduction de risque est encore suffisant ou non.

17.2 Exigences

17.2.1 Avant d'effectuer une modification quelconque à un système instrumenté de sécurité, les procédures d'autorisation et de contrôle des modifications doivent être en place.

17.2.2 Les procédures doivent inclure une méthode claire pour identifier le travail requis et les dangers qui peuvent être pris en compte.

17.2.3 Une analyse doit être effectuée pour déterminer l'impact sur la sécurité fonctionnelle, du fait de la modification proposée. Lorsque l'analyse montre que la modification proposée aura une incidence sur la sécurité, il doit y avoir un retour à la première phase du cycle de vie de sécurité affecté par la modification.

17.2.4 L'activité de modification ne doit pas commencer sans une autorisation appropriée.

17.2.5 Les informations adéquates doivent être maintenues pour toutes les modifications du SIS. Ces informations doivent comprendre:

- une description de la modification ou du changement;
- la raison du changement;
- les dangers identifiés pouvant être pris en compte;
- une analyse de l'impact de l'activité de modification sur le SIS;
- toutes les approbations requises pour les changements;
- les essais utilisés pour vérifier que la modification a été correctement mise en oeuvre et que le SIS fonctionne comme cela est prescrit;
- un historique de la configuration ad hoc;
- les essais utilisés pour vérifier que la modification n'a pas entraîné d'effet néfaste sur des parties du SIS qui n'ont pas été modifiées.

a) description of the tests and inspections performed;

b) dates of the tests and inspections;

c) name of the person(s) who performed the tests and inspections;

d) serial number or other unique identifier of the system tested (for example, loop number, tag number, equipment number, and SIF number);

e) results of the tests and inspection (for example, “as-found” and “as-left” conditions).

17 SIS modification

17.1 Objectives

17.1.1 The objectives of the requirements of this clause are:

- that modifications to any safety instrumented system are properly planned, reviewed and approved prior to making the change; and
- to ensure that the required safety integrity of the SIS is maintained despite of any changes made to the SIS.

NOTE Modifications to the BPCS, other equipment, process or operating conditions should be reviewed to determine whether they are such that the nature or frequency of demands on the SIS will be affected. Those having an adverse effect should be considered further to determine whether the level of risk reduction will still be sufficient.

17.2 Requirements

17.2.1 Prior to carrying out any modification to a safety instrumented system, procedures for authorizing and controlling changes shall be in place.

17.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and the hazards which may be affected.

17.2.3 An analysis shall be carried out to determine the impact on functional safety as a result of the proposed modification. When the analysis shows that the proposed modification will impact safety then there shall be a return to the first phase of the safety life cycle affected by the modification.

17.2.4 Modification activity shall not begin without proper authorization.

17.2.5 Appropriate information shall be maintained for all changes to the SIS. The information shall include

- a description of the modification or change;
- the reason for the change;
- identified hazards which may be affected;
- an analysis of the impact of the modification activity on the SIS;
- all approvals required for the changes;
- tests used to verify that the change was properly implemented and the SIS performs as required;
- appropriate configuration history;
- tests used to verify that the change has not adversely impacted parts of the SIS which were not modified.

17.2.6 La modification doit être effectuée avec du personnel qualifié, qui a été correctement formé. Il convient de notifier à tout le personnel concerné et qui a à en connaître, la nature de la modification et de le former à cette dernière.

18 Déclassement du SIS

18.1 Objectifs

18.1.1 Les objectifs des exigences de cet article sont:

- assurer qu'avant le déclassement du service actif de tout système instrumenté de sécurité, une revue appropriée est conduite et l'autorisation requise est obtenue; et
- assurer que les fonctions instrumentées de sécurité requises demeurent opérationnelles pendant les activités de déclassement.

18.2 Exigences

18.2.1 Avant d'effectuer un déclassement quelconque d'un système instrumenté de sécurité, les procédures d'autorisation et de contrôle des modifications doivent être en place.

18.2.2 Les procédures doivent inclure une méthode claire pour identifier le travail requis et identifier les dangers devant être pris en compte.

18.2.3 Une analyse doit être effectuée pour déterminer l'impact sur la sécurité fonctionnelle, du fait de l'activité de déclassement proposée. L'évaluation doit inclure une mise à jour de l'évaluation de danger et de risque, suffisante pour déterminer l'étendue et la profondeur, que les phases ultérieures du cycle de vie de sécurité doivent avoir besoin de couvrir. L'évaluation doit considérer également:

- la sécurité fonctionnelle pendant l'exécution des activités de déclassement; et
- l'impact du déclassement d'un système instrumenté de sécurité sur les unités fonctionnelles adjacentes et les services d'une installation adjacente.

18.2.4 Les résultats de l'analyse d'impact doivent être utilisés lors de la planification de la sécurité, pour réactiver les exigences appropriées de cette norme, y compris la revérification et la revalidation.

18.2.5 L'activité de déclassement ne doit pas commencer sans une autorisation appropriée.

19 Exigences relatives aux informations et à la documentation

19.1 Objectifs

19.1.1 Les objectifs des exigences de cet article sont:

- assurer que les informations nécessaires sont disponibles et documentées, afin que toutes les phases du cycle de vie de sécurité puissent être effectivement exécutées; et
- assurer que les informations nécessaires sont disponibles et documentées, afin que la vérification, la validation et les activités d'évaluation de la sécurité fonctionnelle puissent être effectivement exécutées.

NOTE 1 Des exemples de structure de documentation sont donnés par l'Annexe A de la CEI 61508-1 et pour plus de détails voir la CEI 61506.

NOTE 2 La documentation peut être disponible sous différentes formes (par exemple, sur papier, film ou tout support d'informations permettant une présentation sur des écrans ou des afficheurs).

17.2.6 Modification shall be performed with qualified personnel who have been properly trained. All affected and appropriate personnel should be notified of the change and trained with regard to the change.

18 SIS decommissioning

18.1 Objectives

18.1.1 The objectives of the requirements of this clause are:

- to ensure that prior to decommissioning any safety instrumented system from active service, a proper review is conducted and required authorization is obtained; and
- to ensure that the required safety instrumented functions remain operational during decommissioning activities.

18.2 Requirements

18.2.1 Prior to carrying out any decommissioning of a safety instrumented system, procedures for authorizing and controlling changes shall be in place.

18.2.2 The procedures shall include a clear method of identifying and requesting the work to be done and identifying the hazards which may be affected.

18.2.3 An analysis shall be carried out on the impact on functional safety as a result of the proposed decommissioning activity. The assessment shall include an update of the hazard and risk assessment sufficient to determine the breadth and depth that subsequent safety life-cycle phases shall need to be re-taken. The assessment shall also consider

- functional safety during the execution of the decommissioning activities; and
- the impact of decommissioning a safety instrumented system on adjacent operating units and facility services.

18.2.4 The results of the impact analysis shall be used during safety planning to re-activate the relevant requirements of this standard including re-verification and re-validation.

18.2.5 Decommissioning activities shall not begin without proper authorization.

19 Information and documentation requirements

19.1 Objectives

19.1.1 The objectives of the requirements of this clause are:

- to ensure that the necessary information is available and documented in order that all phases of the safety life cycle can be effectively performed; and
- to ensure that the necessary information is available and documented in order that verification, validation and functional safety assessment activities can be effectively performed.

NOTE 1 For examples of documentation structure, see IEC 61508-1 Annex A and, for more details, IEC 61506.

NOTE 2 The documentation could be available in different forms (for example, on paper, film or any data medium to be presented on screens or displays).

19.2 Exigences

19.2.1 La documentation requise par cette norme doit être disponible.

19.2.2 Il convient que la documentation:

- décrive l'installation, le système ou les équipements et leur utilisation;
- soit précise;
- soit facile à comprendre;
- réponde à l'objectif pour lequel elle a été prévue; et
- soit disponible sous une forme accessible et pouvant être maintenue.

19.2.3 La documentation doit avoir des identités uniques, ainsi il doit être possible de se référer aux différentes parties.

19.2.4 La documentation doit avoir des désignations indiquant le type d'informations.

19.2.5 La documentation doit être traçable par rapport aux exigences de cette norme.

19.2.6 La documentation doit avoir un index de révision (numéros de version) pour permettre d'identifier les différentes versions des informations.

19.2.7 La documentation doit être structurée pour permettre de rechercher les informations voulues. Il doit être possible d'identifier la dernière révision (version) d'un document.

NOTE Il convient que la structure physique de la documentation puisse changer en fonction d'un certain nombre de facteurs, tels que la taille du système, sa complexité et les exigences d'organisation.

19.2.8 Toute documentation pertinente doit être mise à jour, modifiée, revue, approuvée et être placée sous la maîtrise d'un plan de contrôle ad hoc des informations.

19.2.9 La documentation courante concernant les sujets suivants doit être maintenue:

a) les résultats de l'évaluation de danger et de risque et les hypothèses associées;
b) les équipements utilisés pour les fonctions instrumentées de sécurité, ainsi que leurs exigences concernant la sécurité;
c) l'organisation responsable du maintien de la sécurité fonctionnelle;
d) les procédures nécessaires pour obtenir et maintenir la sécurité fonctionnelle du SIS;
e) les informations de modification, comme cela est défini en 17.2.5;
f) la conception, la mise en oeuvre, les essais et la validation.

NOTE D'autres détails des exigences concernant les informations sont inclus dans les Articles 14 et 15.

19.2 Requirements

19.2.1 The documentation required by this standard shall be available.

19.2.2 The documentation should

- describe the installation, system or equipment and the use of it;
- be accurate;
- be easy to understand;
- suit the purpose for which it is intended; and
- be available in an accessible and maintainable form.

19.2.3 The documentation shall have unique identities so it shall be possible to reference the different parts.

19.2.4 The documentation shall have designations indicating the type of information.

19.2.5 The documentation shall be traceable to the requirements of this standard.

19.2.6 The documentation shall have a revision index (version numbers) to make it possible to identify different versions of the information.

19.2.7 The documentation shall be structured to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document.

NOTE The physical structure of the documentation should vary depending upon a number of factors such as the size of the system, its complexity and the organizational requirements.

19.2.8 All relevant documentation shall be revised, amended, reviewed, approved and be under the control of an appropriate information control scheme.

19.2.9 Current documentation pertaining to the following shall be maintained:

a) the results of the hazard and risk assessment and the related assumptions;
b) the equipment used for safety instrumented functions together with its safety requirements;
c) the organization responsible for maintaining functional safety;
d) the procedures necessary to achieve and maintain functional safety of the SIS;
e) the modification information as defined in 17.2.5;
f) design, implementation, test and validation.

NOTE Further details of the requirements for information are included in Clauses 14 and 15.

ANNEXE A
(informative)

Différences

Cette annexe illustre les différences principales entre la CEI 61511 et la CEI 61508.

La CEI 61511 comporte quelques différences par rapport à la CEI 61508. Ces différences sont présentées aux Articles A.1 et A.2 et sont basées sur la comparaison de cette version de la CEI 61511 avec la CEI 61508.

A.1 Différences organisationnelles

CEI 61508	CEI 61511	Commentaires
Partie 1	Partie 1	Les CEI 61508-1, -2, -3, et -4 ont été combinées en 61511-1
Partie 2	Partie 1	Incluse dans la 61511-1
Partie 3	Partie 1	Incluse dans la 61511-1
Partie 4	Partie 1	Incluse dans la 61511-1
Partie 5	Partie 3	Incluse dans la 61511-3
Partie 6	Partie 2	Directives pour la 61511-1
Partie 7	Toutes les parties	Références informatives incluses dans chaque partie, en tant qu'annexes (si requis).

A.2 Terminologie

CEI 61508-4	CEI 61511-1	Commentaires
Système E/E/PE relatif à la sécurité	SIS	La CEI 61508 se rapporte aux systèmes E/E/PE relatifs à la sécurité, tandis que la CEI 61511 se rapporte aux systèmes instrumentés de sécurité.
PES	SIS	Le «PES» de la CEI 61508 inclut les capteurs et les éléments terminaux de commande, alors que la CEI 61511 utilise le terme SIS.
Système de commande de processus	Système de commande de processus de base	Le système de commande de processus de base est un terme global du domaine des processus.
EUC	Processus	La CEI 61508 se réfère à l'EUC (matériel commandé), tandis que la CEI 61511 se réfère au processus.
Fonction de sécurité	Fonction instrumentée de sécurité (SIF)	Fonction de sécurité de la CEI 61508 mise en oeuvre par le E/E/PES, systèmes relatifs à la sécurité basés sur une autre technologie, ou dispositifs externes de réduction de risque. La SIF de la CEI 61511 n'est mise en oeuvre que par le SIS.

Annex A
(informative)

Differences

This annex illustrates the key differences between IEC 61511 and IEC 61508.

IEC 61511 has some differences from IEC 61508. These differences are discussed in Clauses A.1 and A.2 and are based on the comparison of this version of IEC 61511 to IEC 61508.

A.1 Organizational differences

IEC 61508	IEC 61511	Comment
Part 1	Part 1	IEC 61508-1, -2, -3, and -4 have been combined into IEC 61511-1
Part 2	Part 1	Included in IEC 61511-1
Part 3	Part 1	Included in IEC 61511-1
Part 4	Part 1	Included in IEC 61511-1
Part 5	Part 3	Included in IEC 61511-3
Part 6	Part 2	Guidelines for IEC 61511-1
Part 7	All parts	Informative references included in each part as annexes (where required)

A.2 Terminology

IEC 61508-4	IEC 61511-1	Comment
E/E/PE safety related system	SIS	IEC 61508 refers to E/E/PE safety related systems while IEC 61511 refers to safety instrumented systems
PES	SIS	IEC 61508 “PES” includes sensors and final control elements, while IEC 61511 uses the term SIS.
Process control system	Basic process control system	Basic process control system is a global term for the process sector
EUC	Process	IEC 61508 refers to EUC (equipment under control) while IEC 61511 refers to process
Safety function	Safety instrumented function (SIF)	IEC 61508 safety function implemented by E/E/PES, other technology safety related system, or external risk reduction facilities. IEC 61511 SIF is implemented solely by SIS

Bibliographie

CEI 60050(191):1990, *Vocabulaire Electrotechnique International – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60050(351):1998, *Vocabulaire Electrotechnique International – Partie 351: Commande et régulation automatiques*

CEI 60617-12:1997, *Symboles graphiques pour schémas – Partie 12: Opérateurs logiques binaires*

CEI 61131-3:1993, *Automates programmables – Partie 3: Langages de programmation*

CEI 61506:1997, *Mesure et commande dans les processus industriels – Documentation des logiciels d'application*

CEI 61508-1:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 61508-4:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 4: Définition et abréviations*

CEI 61508-6:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

CEI 61511-3:2003, *Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 3: Conseils pour la détermination des niveaux d'intégrité de sécurité requis*

ISO/IEC 2382 (toutes les parties), *Technologies de l'information – Vocabulaire*

ISO/IEC 2382-1:1993, *Technologies de l'information – Vocabulaire – Partie 1: Termes fondamentaux*

ISO/CEI Guide 51:1999, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*

ISO 9000:2000, *Systèmes de management de la qualité – Principes essentiels et vocabulaire*

ISO 9000-3:1997, *Normes pour le management de la qualité et l'assurance de la qualité – Partie 3: Lignes directrices pour l'application de l'ISO 9001:1994 au développement, à la mise à disposition, à l'installlation et à la maintenance du logiciel*

———————

Bibliography

IEC 60050(191): 1990, *International Electrotechnical Vocabulary – Chapter 191: Dependability and quality of service*

IEC 60050(351):1998, *International Electrotechnical Vocabulary – Part 351: Automatic control*

IEC 60617-12:1997, *Graphical symbols for diagrams – Part 12: Binary logic elements*

IEC 61131-3:1993, *Programmable controllers – Part 3: Programming language*

IEC 61506:1997, *Industrial-process measurement and control – Documentation of application software*

IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 1: General requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 4: Definitions and abbreviations*

IEC 61508-6:2000, *Functional safety of electrical/electronic/programmable electronic safety related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61511-3: 2003, *Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*

ISO/IEC 2382 (all parts), *Information technology – Vocabulary*

ISO/IEC 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*

ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

ISO 9000: 2000, *Quality management systems – Fundamentals and vocabulary*

ISO 9000-3:1997, *Quality management and quality assurance standards – Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software*

———————

Standards Survey

The IEC would like to offer you the best quality standards possible. To make sure that we continue to meet your needs, your feedback is essential. Would you please take a minute to answer the questions overleaf and fax them to us at +41 22 919 03 00 or mail them to the address below. Thank you!

Customer Service Centre (CSC)

International Electrotechnical Commission
3, rue de Varembé
1211 Genève 20
Switzerland

or

Fax to: **IEC**/CSC at +41 22 919 03 00

Thank you for your contribution to the standards-making process.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Customer Service Centre (CSC)
International Electrotechnical Commission
3, rue de Varembé
1211 GENEVA 20
Switzerland

Q1 Please report on **ONE STANDARD** and **ONE STANDARD ONLY**. Enter the exact number of the standard: *(e.g. 60601-1-1)*

.....

Q2 Please tell us in what capacity(ies) you bought the standard *(tick all that apply).* I am the/a:

purchasing agent ❑
librarian ❑
researcher ❑
design engineer ❑
safety engineer ❑
testing engineer ❑
marketing specialist ❑
other.....

Q3 I work for/in/as a: *(tick all that apply)*

manufacturing ❑
consultant ❑
government ❑
test/certification facility ❑
public utility ❑
education ❑
military ❑
other.....

Q4 This standard will be used for: *(tick all that apply)*

general reference ❑
product research ❑
product design/development ❑
specifications ❑
tenders ❑
quality assessment ❑
certification ❑
technical documentation ❑
thesis ❑
manufacturing ❑
other.....

Q5 This standard meets my needs: *(tick one)*

not at all ❑
nearly ❑
fairly well ❑
exactly ❑

Q6 If you ticked NOT AT ALL in Question 5 the reason is: *(tick all that apply)*

standard is out of date ❑
standard is incomplete ❑
standard is too academic ❑
standard is too superficial ❑
title is misleading ❑
I made the wrong choice ❑
other .....

Q7 Please assess the standard in the following categories, using the numbers:
(1) unacceptable,
(2) below average,
(3) average,
(4) above average,
(5) exceptional,
(6) not applicable

timeliness.....
quality of writing.....
technical contents.....
logic of arrangement of contents .....
tables, charts, graphs, figures.....
other .....

Q8 I read/use the: *(tick one)*

French text only ❑
English text only ❑
both English and French texts ❑

Q9 Please share any comment on any aspect of the IEC that you would like us to know:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Enquête sur les normes

La CEI ambitionne de vous offrir les meilleures normes possibles. Pour nous assurer que nous continuons à répondre à votre attente, nous avons besoin de quelques renseignements de votre part. Nous vous demandons simplement de consacrer un instant pour répondre au questionnaire ci-après et de nous le retourner par fax au +41 22 919 03 00 ou par courrier à l'adresse ci-dessous. Merci !

Centre du Service Clientèle (CSC)

Commission Electrotechnique Internationale
3, rue de Varembé
1211 Genève 20
Suisse

ou

Télécopie: **CEI**/CSC +41 22 919 03 00

Nous vous remercions de la contribution que vous voudrez bien apporter ainsi à la Normalisation Internationale.

Nicht frankieren
Ne pas affranchir

Non affrancare
No stamp required

A Prioritaire

RÉPONSE PAYÉE

SUISSE

Centre du Service Clientèle (CSC)
Commission Electrotechnique Internationale
3, rue de Varembé
1211 GENÈVE 20
Suisse

Q1 Veuillez ne mentionner qu'**UNE SEULE NORME** et indiquer son numéro exact: (*ex. 60601-1-1)*

.....

Q2 En tant qu'acheteur de cette norme, quelle est votre fonction?
(cochez tout ce qui convient)
Je suis le/un:

agent d'un service d'achat ❑
bibliothécaire ❑
chercheur ❑
ingénieur concepteur ❑
ingénieur sécurité ❑
ingénieur d'essais ❑
spécialiste en marketing ❑
autre(s).....

Q3 Je travaille:
(cochez tout ce qui convient)

dans l'industrie ❑
comme consultant ❑
pour un gouvernement ❑
pour un organisme d'essais/ certification ❑
dans un service public ❑
dans l'enseignement ❑
comme militaire ❑
autre(s).....

Q4 Cette norme sera utilisée pour/comme
(cochez tout ce qui convient)

ouvrage de référence ❑
une recherche de produit ❑
une étude/développement de produit ❑
des spécifications ❑
des soumissions ❑
une évaluation de la qualité ❑
une certification ❑
une documentation technique ❑
une thèse ❑
la fabrication ❑
autre(s).....

Q5 Cette norme répond-elle à vos besoins:
(une seule réponse)

pas du tout ❑
à peu près ❑
assez bien ❑
parfaitement ❑

Q6 Si vous avez répondu PAS DU TOUT à Q5, c'est pour la/les raison(s) suivantes:
(cochez tout ce qui convient)

la norme a besoin d'être révisée ❑
la norme est incomplète ❑
la norme est trop théorique ❑
la norme est trop superficielle ❑
le titre est équivoque ❑
je n'ai pas fait le bon choix ❑
autre(s) .....

Q7 Veuillez évaluer chacun des critères ci-dessous en utilisant les chiffres
(1) inacceptable,
(2) au-dessous de la moyenne,
(3) moyen,
(4) au-dessus de la moyenne,
(5) exceptionnel,
(6) sans objet

publication en temps opportun .....
qualité de la rédaction.....
contenu technique .....
disposition logique du contenu .....
tableaux, diagrammes, graphiques, figures.....
autre(s) .....

Q8 Je lis/utilise: *(une seule réponse)*

uniquement le texte français ❑
uniquement le texte anglais ❑
les textes anglais et français ❑

Q9 Veuillez nous faire part de vos observations éventuelles sur la CEI:

.....
.....
.....
.....
.....
.....

ISBN 2-8318-7316-9

ICS 25.040.01; 13.110

Typeset and printed by the IEC Central Office
GENEVA, SWITZERLAND